



(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 I676945 B

(45)公告日：中華民國 108 (2019) 年 11 月 11 日

(21)申請案號：105107433

(22)申請日：中華民國 105 (2016) 年 03 月 10 日

(51)Int. Cl. : G06Q20/22 (2012.01)

G06Q20/30 (2012.01)

(30)優先權：2015/09/11 中國大陸

201510578511.6

(71)申請人：香港商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：吳超 (CN)；單斌 (CN)；周曉愷 (CN)；王曉晨 (CN)

(74)代理人：林志剛

(56)參考文獻：

TW M467132

US 8,459,545B1

US 2010/0138908A1

US 2012/0143768A1

US 2012/0216042A1

US 2014/0236842A1

US 2014/0299660A1

審查人員：趙齊祥

申請專利範圍項數：50 項 圖式數：19 共 53 頁

(54)名稱

綁定可穿戴設備的方法和裝置、電子支付方法和裝置

(57)摘要

本發明提供一種綁定可穿戴設備的方法，應用在可穿戴設備上，包括：向終端提供本設備的設備資訊；所述設備資訊包括設備標識，供終端向伺服器發送設備標識和使用終端的用戶帳戶；接收來自伺服器的設備憑證，所述設備憑證由伺服器根據設備標識產生，並與所述用戶帳戶具有對應關係；將設備憑證保存在本地，用來通過對應的用戶帳戶進行支付。通過本發明的技術方案，即使在用戶使用的可穿戴設備與終端之間、或終端與伺服器之間的通信都斷開時，仍能通過可穿戴設備完成支付，提高了支付成功率，增加了用戶便利程度。

指定代表圖：

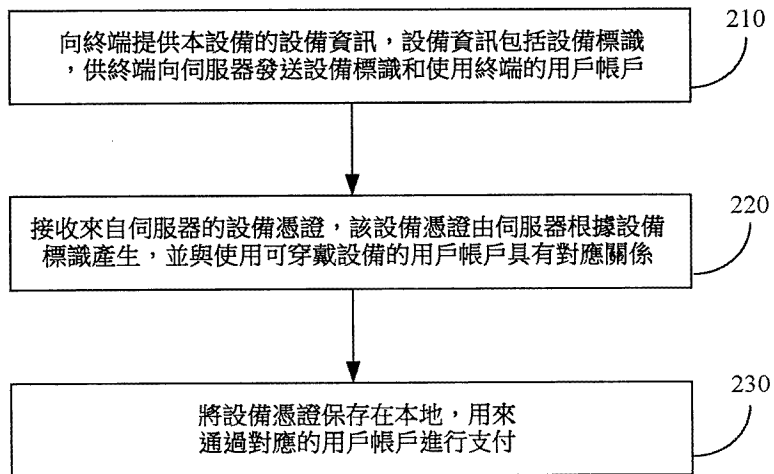


圖 2

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)

綁定可穿戴設備的方法和裝置、電子支付方法和裝置

【技術領域】

本發明涉及網路通信技術領域，尤其涉及一種綁定可穿戴設備的方法和裝置、一種電子支付方法和裝置。

【先前技術】

可穿戴設備是一種可被用戶穿戴在身上，或整合到用戶衣服或配件中的攜帶型設備，如手環、智慧手錶、智慧運動鞋、智慧服裝、智慧眼鏡、智慧頭盔、智慧戒指等。可穿戴設備具有計算功能，可以通過硬體介面或無線區域網連接到智慧手機、平板電腦、個人電腦等終端，通過與終端交換資料來實現各種功能。

可穿戴設備可以用來進行電子支付。現有技術中，在用戶希望用可穿戴設備進行支付時，先通過手機向提供支付業務功能的伺服器請求付款碼；伺服器產生用於本次支付的付款碼發送給手機，並記錄付款碼和使用手機的用戶帳戶的對應關係；手機將收到的付款碼轉發給可穿戴設備，由可穿戴設備進行顯示；商戶的收款設備掃描付款碼，將付款碼、支付金額和其他交易資訊發送到伺服器；伺服器從付款碼對應的用戶帳戶扣除支付金額的款項，轉

入該商戶的帳戶中，從而完成支付。

上述支付過程中，當可穿戴設備與手機之間的連接狀態不好，或者手機與伺服器之間的網路性能較差時，常常會導致可穿戴設備無法得到付款碼或者不能及時顯示付款碼，造成支付失敗。

【發明內容】

有鑒於此，本發明提供一種綁定可穿戴設備的方法，應用在可穿戴設備上，包括：

向終端提供本設備的設備資訊；所述設備資訊包括設備標識，供終端向伺服器發送設備標識和使用終端的用戶帳戶；

接收來自伺服器的設備憑證，所述設備憑證由伺服器根據設備標識產生，並與所述用戶帳戶具有對應關係；

將設備憑證保存在本地，用來通過對應的用戶帳戶進行支付。

本發明提供的一種綁定可穿戴設備的方法，應用在伺服器上，包括：

接收終端發送的綁定請求；所述綁定請求中包括可穿戴設備的設備標識和使用終端的用戶帳戶；

根據設備標識產生可穿戴設備的設備憑證，保存設備憑證與所述用戶帳戶的對應關係；

將設備憑證提供給可穿戴設備，供可穿戴設備通過對應的用戶帳戶進行支付。

本發明提供的一種綁定可穿戴設備的方法，應用在終端上，包括：

獲取可穿戴設備的設備資訊，其中包括可穿戴設備的設備標識；

向伺服器發送綁定請求；所述綁定請求中包括可穿戴設備的設備標識和使用本終端的用戶帳戶，供伺服器產生對應於用戶帳戶的設備憑證並提供給可穿戴設備；所述設備憑證由可穿戴設備用來通過對應的用戶帳戶進行支付。

本發明提供的一種電子支付方法，應用在可穿戴設備上，所述可穿戴設備上保存有對應於用戶帳戶的設備憑證，所述方法包括：

收到用戶的指令後，根據保存的設備憑證產生交易憑證；

向收款方設備提供交易憑證，供收款方設備上傳到伺服器，在還原出設備憑證後以對應的用戶帳戶進行支付。

本發明提供的一種電子支付方法，應用在伺服器上，所述伺服器可以獲得可穿戴設備的設備憑證和使用所述可穿戴設備的用戶帳戶的對應關係，所述方法包括：

接收收款方設備發送的收款請求，收款請求中包括由可穿戴設備產生的交易憑證和款項資訊；

根據交易憑證還原所述可穿戴設備的設備憑證；

按照款項資訊，以所述設備憑證對應的用戶帳戶作為支付方完成支付。

本發明提供的一種電子支付方法，應用在收款方設備

上，包括：

獲取可穿戴設備的交易憑證；所述交易憑證由可穿戴設備根據其對應於用戶帳戶的設備憑證產生；

向伺服器發送收款請求；收款請求中包括可穿戴設備的交易憑證和款項資訊，供伺服器由交易憑證還原出設備憑證，按照款項資訊以對應於設備憑證的用戶帳戶進行支付。

本發明還提供了一種綁定可穿戴設備的裝置，應用在可穿戴設備上，包括：

設備資訊提供單元，用於向終端提供本設備的設備資訊；所述設備資訊包括設備標識，供終端向伺服器發送設備標識和使用終端的用戶帳戶；

設備憑證接收單元，用於接收來自伺服器的設備憑證，所述設備憑證由伺服器根據設備標識產生，並與所述用戶帳戶具有對應關係；

設備憑證保存單元，用於將設備憑證保存在本地，用來通過對應的用戶帳戶進行支付。

本發明提供的一種綁定可穿戴設備的裝置，應用在伺服器上，包括：

綁定請求接收單元，用於接收終端發送的綁定請求；所述綁定請求中包括可穿戴設備的設備標識和使用終端的用戶帳戶；

設備憑證產生單元，用於根據設備標識產生可穿戴設備的設備憑證，保存設備憑證與所述用戶帳戶的對應關

係；

設備憑證下發單元，用於將設備憑證提供給可穿戴設備，供可穿戴設備通過對應的用戶帳戶進行支付。

本發明提供的一種綁定可穿戴設備的裝置，應用在終端上，包括：

設備資訊獲取單元，用於獲取可穿戴設備的設備資訊，其中包括可穿戴設備的設備標識；

綁定請求發送單元，用於向伺服器發送綁定請求；所述綁定請求中包括可穿戴設備的設備標識和使用本終端的用戶帳戶，供伺服器產生對應於用戶帳戶的設備憑證並提供給可穿戴設備；所述設備憑證由可穿戴設備用來通過對應的用戶帳戶進行支付。

本發明提供的一種電子支付裝置，應用在可穿戴設備上，所述可穿戴設備上保存有對應於用戶帳戶的設備憑證，所述裝置包括：

交易憑證產生單元，用於在收到用戶的指令後，根據保存的設備憑證產生交易憑證；

交易憑證提供單元，用於向收款方設備提供交易憑證，供收款方設備上傳到伺服器，在還原出設備憑證後以對應的用戶帳戶進行支付。

本發明提供的一種電子支付裝置，應用在伺服器上，所述伺服器可以獲得可穿戴設備的設備憑證和使用所述可穿戴設備的用戶帳戶的對應關係，所述裝置包括：

收款請求接收單元，用於接收收款方設備發送的收款

請求，收款請求中包括由可穿戴設備產生的交易憑證和款項資訊；

設備憑證還原單元，用於根據交易憑證還原所述可穿戴設備的設備憑證；

支付單元，用於按照款項資訊，以所述設備憑證對應的用戶帳戶作為支付方完成支付。

本發明提供的一種電子支付裝置，應用在收款方設備上，包括：

交易憑證獲取單元，用於獲取可穿戴設備的交易憑證；所述交易憑證由可穿戴設備根據其對應於用戶帳戶的設備憑證產生；

收款請求發送單元，用於向伺服器發送收款請求；收款請求中包括可穿戴設備的交易憑證和款項資訊，供伺服器由交易憑證還原出設備憑證，按照款項資訊以對應於設備憑證的用戶帳戶進行支付。

由以上技術方案可見，本發明的實施例中，在可穿戴設備上保存伺服器產生的設備憑證，在伺服器側建立設備憑證與用戶帳戶的對應關係，可穿戴設備利用設備憑證即可進行支付流程，不再需要即時從終端或從伺服器接收付款碼，從而即使在用戶使用的可穿戴設備與終端之間、或終端與伺服器之間的通信都斷開時，仍能通過可穿戴設備完成支付，提高了支付成功率，增加了用戶便利程度。

【圖式簡單說明】

圖 1 是本發明實施例一中一種應用場景的網路結構圖；

圖 2 是本發明實施例一中應用在可穿戴設備上的綁定可穿戴設備的方法的流程圖；

圖 3 是本發明實施例一中應用在伺服器上的綁定可穿戴設備的方法的流程圖；

圖 4 是本發明實施例一中應用在終端上的綁定可穿戴設備的方法的流程圖；

圖 5 是本發明實施例二中一種應用場景的網路結構圖；

圖 6 是本發明實施例二中應用在可穿戴設備上的電子支付方法的流程圖；

圖 7 是本發明實施例二中應用在伺服器上的電子支付方法的流程圖；

圖 8 是本發明實施例二中應用在收款方設備上的電子支付方法的流程圖；

圖 9 是本發明應用示例中綁定可穿戴設備時可穿戴設備、終端與伺服器之間的互動流程圖；

圖 10 是終端上一種啟動智慧手錶綁定流程的介面示例圖；

圖 11 是一種終端上提示用戶掃描智慧手錶以獲取設備資訊的介面示例圖；

圖 12 是本發明應用示例中支付時可穿戴設備、收款方終端與伺服器之間的互動流程圖；

圖 13 是可穿戴設備、終端或伺服器的一種硬體結構圖；

圖 14 是本發明實施例中一種應用在可穿戴設備上的綁定可穿戴設備的裝置的邏輯結構圖；

圖 15 是本發明實施例中一種應用在伺服器上的綁定可穿戴設備的裝置的邏輯結構圖；

圖 16 是本發明實施例中一種應用在終端上的綁定可穿戴設備的裝置的邏輯結構圖；

圖 17 是本發明實施例中一種應用在可穿戴設備上的電子支付裝置的邏輯結構圖；

圖 18 是本發明實施例中一種應用在伺服器上的電子支付裝置的邏輯結構圖；

圖 19 是本發明實施例中一種應用在收款方設備上的電子支付裝置的邏輯結構圖。

【實施方式】

現有技術中，伺服器通過即時產生的付款碼將某次支付的付款方對應於請求該付款碼的用戶帳戶。由於可穿戴設備通常專屬於一個用戶，本發明的實施例中，在可穿戴設備上保存和用戶帳戶對應的設備憑證，利用該設備憑證通過收款方設備發起支付；伺服器側通過設備憑證和用戶帳戶的對應關係，來獲知支付的付款方帳戶。這樣在支付過程中，只要收款方設備與伺服器之間能夠正常通信，即可完成支付，避免了可穿戴設備與終端之間、終端與伺服

器之間的網路性能下降對支付的影響，從而解決現有技術中存在的問題。

本發明的實施例中，伺服器用來實現支付業務功能，可以是一個實體或邏輯伺服器，也可以是由兩個或兩個以上分擔不同職責的實體或邏輯伺服器、相互協同來實現本發明實施例中伺服器的各項功能。

本發明的實施例一提出一種綁定可穿戴設備的方法，所應用的一種網路環境如圖 1 所示。可穿戴設備通過硬體介面或無線區域網存取到終端，硬體介面可以是音頻介面、USB（Universal Serial Bus，通用串列匯流排）介面等，無線區域網可以是藍牙（Bluetooth）、Wi-Fi（Wireless-Fidelity，無線保真）、ZigBee（紫蜂協定）等，終端可以是智慧手機、平板電腦、個人電腦等。終端通過通信網路（如網際網路和/或移動通信網路）與伺服器進行通信；在一些應用場景中，具有相應功能的可穿戴設備也可以通過 Wi-Fi、移動通信網路等與伺服器直接通信。本實施例中對終端的種類、可穿戴設備存取終端的硬體介面或無線區域網協定、通信網路的協定和組網結構、伺服器的具體實現方式等均不做限定。

實施例一中，綁定可穿戴設備的方法應用在可穿戴設備上的流程如圖 2 所示，應用在伺服器上的流程如圖 3 所示，應用在終端上的流程如圖 4 所示。

在可穿戴設備上，步驟 210，向終端提供本設備的設備資訊，設備資訊包括設備標識，供終端向伺服器發送設

備標識和使用終端的用戶帳戶。

在終端上，步驟 410，獲取可穿戴設備的設備資訊，其中包括可穿戴設備的設備標識。

可穿戴設備的設備標識用來唯一代表該穿戴設備，因具體的設備種類、生產廠商和採用的無線區域網協定的不同而不同，通常可以是該可穿戴設備的硬體位址，如 MAC (Media Access Control，媒體存取控制) 位址，也可以是生產廠商賦予該可穿戴設備的識別碼，如蘋果設備的 UUID (Universally Unique Identifier，通用唯一識別碼)。可穿戴設備的設備資訊還可以包括可穿戴設備的硬體型號或系統軟體版本資訊、與終端之間可採用的連接方式和連接參數等。

可穿戴設備可以在收到用戶的預定操作後，將本設備的設備資訊提供給終端，也可以根據終端的請求，將本設備的設備資訊發送給終端。

現有技術中，終端的作業系統通常具有基於某種通信協定連接可穿戴設備的功能，終端上的支付用戶端軟體可以利用這一功能從可穿戴設備獲得其設備資訊。但是這種方式需要用戶端軟體的實現因作業系統的不同而不同，不具有通用性。為了避免這一問題，在一種實現方式中，可以由可穿戴設備在收到用戶的預定操作後，產生攜帶設備資訊的二維碼並顯示在螢幕上供終端掃描；終端掃描可穿戴設備顯示的二維碼，從二維碼資訊中得到可穿戴設備的設備資訊。

在終端上，步驟 420，向伺服器發送綁定請求，綁定請求中包括可穿戴設備的設備標識和使用本終端的用戶帳戶，供伺服器產生對應於用戶帳戶的設備憑證並提供給可穿戴設備。

可穿戴設備通常不向用戶提供手動輸入資訊的功能，使用可穿戴設備的用戶（也就是使用終端的用戶）在伺服器上用於支付的用戶帳戶可以在終端上由用戶輸入並保存。終端將用戶帳戶和可穿戴設備的設備標識封裝在綁定請求中，發送給伺服器。

在伺服器上，步驟 310，接收終端發送的綁定請求。

在伺服器上，步驟 320，根據設備標識產生可穿戴設備的設備憑證，保存設備憑證與用戶帳戶的對應關係。

伺服器在收到終端發送的綁定請求後，從中得到可穿戴設備的設備標識和使用該可穿戴設備的用戶帳戶。伺服器以設備標識作為輸入，採用預定的映射演算法得到可穿戴設備的設備憑證。設備憑證可以是包括數位、字母、符號中一種到多種的字串，也可以是數位證書，本實施例不做限定；伺服器可以採用任何能夠將不同的設備標識映射為不同設備憑證的映射演算法，本實施例同樣不做限定。

伺服器將為該可穿戴設備產生的設備憑證與使用該可穿戴設備的用戶帳戶的對應關係保存在可存取的儲存位置，如伺服器本地、通過網路可存取的儲存設備或雲儲存的儲存空間中。

在伺服器上，步驟 330，將設備憑證提供給可穿戴設

備，供可穿戴設備通過對應的用戶帳戶進行支付。

在可穿戴設備上，步驟 220，接收來自伺服器的設備憑證，該設備憑證由伺服器根據設備標識產生，並與使用可穿戴設備的用戶帳戶具有對應關係。

伺服器可以將設備憑證發送給終端，由終端將設備憑證轉發給可穿戴設備。

在一些應用場景中，可穿戴設備可以直接通過 Wi-Fi 或移動通信網路與伺服器進行通信，這樣的場景中，可穿戴設備可以在向終端提供本設備的設備資訊後，向伺服器發送授權請求，授權請求中包括本設備的設備標識；伺服器既收到來自終端的綁定請求，也收到來自可穿戴設備的授權請求，授權請求和綁定請求中都包括可穿戴設備的設備標識；伺服器將為該設備標識產生的設備憑證攜帶在對授權請求的回應中發送可穿戴設備，並保存該設備憑證與綁定請求中用戶帳戶的對應關係；可穿戴設備接收伺服器發送的本設備的設備憑證。

為了增強設備憑證在傳輸過程中的安全性，可以在伺服器向可穿戴設備下發設備憑證的傳輸過程中對設備憑證進行加密。

在一個例子中，在可穿戴設備和伺服器上預置相同或對應的加解密演算法，由可穿戴設備產生用來在傳輸過程中加密設備憑證的設備端密鑰和服務端密鑰，根據所採用的加解密演算法，設備端密鑰與服務端密鑰可以相同，也可以相對應。可穿戴設備將設備端密鑰保存在本地，將服

務端密鑰提供給伺服器。可穿戴設備可以將服務端密鑰發送給終端，由終端將服務端密鑰攜帶在綁定請求中發送給伺服器；伺服器從綁定請求中得到可穿戴設備產生的服務端密鑰，以該服務端密鑰對該可穿戴設備的設備密鑰進行加密後發送給終端，由終端轉發給該可穿戴設備。在可穿戴設備可以直接與伺服器通信的場景中，可穿戴設備可以將服務端密鑰攜帶在授權請求中發送給伺服器；伺服器利用該服務端對該可穿戴設備的設備密鑰進行加密，並向可穿戴設備回覆對授權請求的回應，回應中包括加密後的設備憑證。可穿戴設備接收來自伺服器、經服務端密鑰加密後的設備憑證，利用設備端密鑰進行解密後，得到設備憑證。

在另一個例子中，在可穿戴設備和伺服器上預置相同或對應的加解密演算法，由伺服器產生用來在傳輸過程中加密設備憑證的設備端密鑰和服務端密鑰，並且將設備端密鑰提供給可穿戴設備。伺服器可以將設備端密鑰發送給終端，由終端轉發給可穿戴設備；在伺服器能夠與可穿戴設備直接通信的場景中，也可以直接將設備端密鑰發送給可穿戴設備。

在可穿戴設備上，步驟 230，將設備憑證保存在本地，用來通過對應的用戶帳戶進行支付。

可穿戴設備將伺服器產生的設備憑證保存在本地，即可採用該設備憑證，通過對應於該設備憑證的用戶帳戶來進行電子支付。

可穿戴設備可以在對設備憑證採用加密演算法加密後，將密文保存在本地，以提高設備憑證的安全性。在需要使用設備憑證時，可穿戴設備可以對密文進行解密。在保存設備憑證時的加密和解密都在可穿戴設備本地進行，可以採用可穿戴設備支援的任意加解密演算法；可以與前述傳輸設備憑證時採用的加解密演算法相同，也可以不同，本實施例中均不做限定。

在一些應用場景中，為了增加支付過程的安全性，伺服器可以為每個用戶帳戶產生對應的安全憑證，在下發設備憑證時，一併將安全憑證提供給可穿戴設備。伺服器保存用戶帳戶、設備憑證和安全憑證的對應關係。可穿戴設備收到設備憑證和安全憑證後，一起保存在本地。安全憑證用來在可穿戴設備支付時對設備憑證進行安全校驗，詳細說明請參見實施例二。

實施例一中，伺服器根據可穿戴設備的設備標識產生設備憑證，將設備憑證與終端提供的使用可穿戴設備的用戶帳戶進行綁定，可穿戴設備可以利用伺服器下發的設備憑證來通過對應的用戶帳戶進行支付，使得支付過程不再需要終端參與，避免了終端與可穿戴設備之間、終端與伺服器之間的連接狀況或網路性能對支付過程的影響，提高了支付成功率，為用戶提供更多便利。

本發明的實施例二提出一種電子支付的方法，所應用的一種網路環境如圖 5 所示，可穿戴設備可以通過連接方式或非連接方式與收款方設備進行資料傳輸，其中連接方

式可以是 Wi-Fi、藍牙等，非連接方式可以是掃描等；收款方設備能夠從可穿戴設備獲取資料，並通過通信網路與伺服器進行通信；收款方設備可以是單台設備，也可以是多台設備組合後用於實現上述功能。本實施例對收款方設備的種類和組成、可穿戴設備與收款方設備之間的資料傳輸方式、通信網路的協定和組網結構、伺服器的具體實現方式等均不做限定。

實施例二中，在可穿戴設備上保存有設備憑證，設備憑證與在伺服器上用來進行支付的用戶帳戶具有對應關係，該用戶帳戶屬於使用該可穿戴設備的用戶。可穿戴設備的設備憑證與用戶帳戶的對應關係保存在伺服器可存取的儲存位置。詳細描述請參見實施例一，不再重複。

實施例二中，電子支付的方法應用在可穿戴設備上的流程如圖 6 所示，應用在伺服器上的流程如圖 7 所示，應用在終端上的流程如圖 8 所示。

在可穿戴設備上，步驟 610，收到用戶的指令後，根據保存的設備憑證產生交易憑證。

當用戶希望通過可穿戴設備向收款方支付時，在可穿戴設備上執行啟動支付的操作。可穿戴收到用戶的指令，讀取保存的設備憑證，產生交易憑證。

按照收款方設備的類型和可穿戴設備與收款方設備之間的通信方式，交易憑證可以是字串、證書、二維碼、條碼等。交易憑證將作為支付方的身份資訊上傳到伺服器，由伺服器逆向計算出設備憑證，以該設備憑證對應的用戶

帳戶作為支付方。可以根據實際應用場景中設備憑證和交易憑證的形式來決定產生交易憑證的具體演算法，本實施例中不做限定，只要伺服器上能夠採用逆向演算法根據交易憑證得到設備憑證即可。

在一些實現方式中，可穿戴設備保存的設備憑證是採用加密演算法加密後的設備憑證密文。可穿戴設備讀取保存的設備憑證密文後，用對應的解密演算法進行解密得到設備憑證，再利用設備憑證產生交易憑證。

需要說明的是，本實施例中可穿戴設備具有產生和提供交易憑證所需的硬體和軟體資源。例如，在以二維碼或條碼作為交易憑證的應用場景中，可穿戴設備需要有能夠清晰顯示二維碼或條碼的螢幕、足夠的運算能力和儲存空間等硬體資源，往往還需要有二維碼或條碼軟體工具包等軟體資源。

在可穿戴設備上，步驟 620，向收款方設備提供交易憑證，供收款方設備上傳到伺服器，在還原出設備憑證後以對應的用戶帳戶進行支付。

在收款方設備上，步驟 810，獲取可穿戴設備的交易憑證；該交易憑證由可穿戴設備根據其對應於用戶帳戶的設備憑證產生。

根據可穿戴設備與收款方設備之間的通信方式，可穿戴設備可以基於與收款方設備之間的連接將設備憑證發送給收款方設備，也可以將設備憑證顯示在螢幕上供收款方設備掃描。

在收款方設備上，步驟 820，向伺服器發送收款請求，收款請求中包括可穿戴設備的交易憑證和款項資訊；供伺服器由交易憑證還原出設備憑證，按照款項資訊以對應於設備憑證的用戶帳戶進行支付。

在伺服器上，步驟 710，接收收款方設備發送的收款請求。

收款方設備將款項資訊和從可穿戴設備獲取的交易憑證封裝在收款請求中，發送給伺服器。款項資訊包括支付金額，還可以包括與本次支付有關的其他資訊，如用於交易付款時，還可以包括所交易的商品或服務名稱、數量等。收款請求中還攜帶有收款方帳戶。

在伺服器上，步驟 720，根據交易憑證還原該可穿戴設備的設備憑證。

按照可穿戴設備產生設備憑證的演算法，伺服器採用逆向演算法，由交易憑證還原出可穿戴設備的設備憑證。

在伺服器上，步驟 730，按照款項資訊，以設備憑證對應的用戶帳戶作為支付方完成支付。

從可穿戴設備的設備憑證和用戶帳戶的對應關係的儲存位置，伺服器可以獲得還原出的設備憑證所對應的用戶帳戶是哪個。伺服器從設備憑證對應的用戶帳戶扣除款項資訊確定的金額，支付給收款方帳戶，從而完成支付。

伺服器將是否支付成功的結果返回給收款方設備。

為了增加支付過程的安全性，伺服器可以對可穿戴設備產生的交易憑證進行安全校驗，各種安全校驗方式都可

以用於支付過程，本實施例中不做限定。

在一種實現方式中，伺服器在綁定流程中向可穿戴設備下發設備憑證時，將對應的安全憑證一併下發給可穿戴設備，在本實施例中的支付流程中，可穿戴設備在步驟 610 中，根據保存的設備憑證和安全憑證，利用憑證產生演算法產生帶有校驗資訊的交易憑證；伺服器在步驟 720 中，根據交易憑證，利用憑證還原演算法得到可穿戴設備的設備憑證和安全憑證；其中，可穿戴設備採用的憑證產生演算法與伺服器採用的憑證還原演算法為相對應的逆向演算法。伺服器在步驟 730 中，根據服務端保存的安全憑證和還原出的安全憑證，對交易憑證（或還原出的設備憑證）進行校驗，通過校驗後按照款項資訊，以還原出的設備憑證對應的用戶帳戶作為支付方完成支付。

這種實現方式中，可以根據應用場景的需要來確定所採用的憑證產生演算法、憑證還原演算法，以及與這兩種演算法匹配的安全憑證，本實施例中不做限定。此外，安全憑證可以隨時間變化，以進一步增加校驗的可靠性，具體而言，可穿戴設備可以在綁定流程中與伺服器啟動同步計時，在可穿戴設備和伺服器上預置的相同的安全憑證變化演算法，根據該演算法，安全憑證每隔預定時間在可穿戴設備和伺服器上變更為另一個同樣的值。這樣，可穿戴設備在步驟 610 中產生的交易憑證只在上述預定時間內有效，超過預定時間，由於伺服器上的安全憑證發生變化，將導致交易憑證無法通過安全校驗，而不能完成支付。這

個例子中的安全憑證變化演算法可以參考現有技術中付款碼的產生演算法來實現，此處不再贅述。

在另一種實現方式中，在綁定流程中，伺服器保存可穿戴設備的設備標識、用戶帳戶和設備憑證的對應關係。可穿戴設備根據自身的設備標識、伺服器下發的設備憑證和安全憑證來產生交易憑證。這樣，伺服器可以利用從交易憑證還原出的設備標識，對可穿戴設備本身進行安全校驗。即使設備標識和安全憑證被移植到非法可穿戴設備上，也不會造成用戶的損失。

實施例二中，可穿戴設備利用本地保存的設備憑證產生交易憑證來進行支付；伺服器用交易憑證還原出設備憑證，根據保存的設備憑證與用戶帳戶的對應關係，以對應的用戶帳戶作為支付方來完成支付。可穿戴設備在支付過程中不需要與終端或伺服器直接傳輸資料，可以在離線狀態下進行支付，這樣無論可穿戴設備與終端之間、終端與伺服器之間是否可以通信都不會影響支付，提高了支付成功的概率。

在本發明的一個應用示例中，用戶的智慧手錶可以通過藍牙連接到其終端，終端上和智慧手錶上分別安裝有相同支付平臺的支付用戶端 App（應用程式），終端上的支付 App 可以通過移動通信網路或 Wi-Fi 與該支付平臺的伺服器進行通信。

對應於實施例一，本應用示例中在綁定可穿戴設備時的流程請參見圖 9。

用戶在使用終端的 App 時，需要輸入在伺服器上註冊的用戶帳戶及密碼以登錄。登錄後，用戶可以在終端的支付 App 上啟動綁定智慧手錶的流程。終端上一種可能的介面如圖 10 所示，當用戶點擊“開始綁定”按鈕時，終端上顯示提示用戶接下來如何進行操作的資訊，一種可能的介面如圖 11 所示。

智慧手錶上的支付 App 具有以設備資訊產生二維碼的功能，用戶啟動該功能後，在智慧手錶上顯示攜帶有設備標識和其他設備資訊（包括與可穿戴設備進行藍牙連接的其他連接參數）的二維碼。

用戶用終端掃描智慧手錶上顯示的二維碼，得到智慧手錶的設備資訊。終端提取其中的設備資訊，與可穿戴設備建立藍牙連接。連接成功後，終端向可穿戴設備發送密鑰請求。可穿戴設備採用非對稱加密演算法產生對應的公鑰和私鑰，將私鑰作為設備端密鑰保存在本地，將公鑰作為服務端密鑰在對密鑰請求的回應中發送給終端。

終端將可穿戴設備的設備標識、終端登錄伺服器的用戶帳戶和公鑰封裝在綁定請求中，發送給伺服器。

伺服器根據綁定請求中的設備標識產生設備憑證，為該可穿戴設備指定安全憑證，保存設備憑證、安全憑證與同一個綁定請求中的用戶帳戶的對應關係。伺服器用公鑰對設備憑證進行加密，將加密後的設備憑證和安全憑證封裝在對綁定請求的回應中返回給終端。伺服器在產生設備憑證前，可以要求終端提供用戶帳戶的密碼來進行安全確

認，如果終端不能提供正確的密碼，則綁定流程以失敗結束。

終端收到對綁定請求的回應後，將其中加密後的設備憑證通過藍牙發送給可穿戴設備。

可穿戴設備用保存的私鑰對加密的設備憑證進行解密，得到設備憑證。之後利用預置的加密演算法對設備憑證進行加密，並將加密後的設備憑證密文保存在本地。可穿戴設備與伺服器啟動同步計時，啟動後，根據可穿戴設備和伺服器上預置的相同安全憑證變化演算法，可穿戴設備上保存的安全憑證和伺服器上保存的安全憑證在隨計時時間同步進行相同的變化。至此，可穿戴設備與用戶帳戶的綁定成功，綁定流程結束。

對應於實施例二，本應用示例中在用可穿戴設備進行支付時的流程請參見圖 12。

當用戶希望用可穿戴設備為購買的商品向商戶付款時，在可穿戴設備的支付 App 中啟動支付流程。收到用戶啟動支付的指令後，可穿戴設備從本地的儲存區讀取設備憑證密文，用預置的解密演算法解密後得到設備憑證。利用憑證產生演算法，可穿戴設備以匹配於當前計時時間的安全憑證和設備憑證為輸入，得到帶有校驗資訊的交易憑證，交易憑證採用條碼形式，可穿戴設備將條碼顯示在螢幕上。

商戶的收款方設備掃描條碼，得到可穿戴設備產生的交易憑證。收款方設備將交易憑證、商品名稱及數量、交

易金額等封裝在收款請求中，發送給伺服器。

伺服器採用憑證還原演算法將交易憑證還原為設備憑證和安全憑證。伺服器比較還原出的安全憑證和服務端匹配於計時時間的安全憑證，如果兩者相同則交易憑證（或還原出的設備憑證）通過校驗，否則支付流程失敗。如果設備憑證通過校驗，則查找與設備憑證具有對應關係的用戶帳戶，以該用戶帳戶為支付方，以該商戶的帳戶為收款方帳戶，完成交易金額款項的支付。當然，在完成支付前，伺服器還可以校驗該商戶的帳戶是否合法，對商戶帳戶的校驗過程本應用示例中與現有技術相同，不再贅述。

伺服器將是否支付成功的通知消息發送給商戶的收款方設備。至此，支付流程結束。

與上述流程實現對應，本發明的實施例還提供了三種分別應用在可穿戴設備、終端和伺服器上的綁定可穿戴設備的裝置，和三種分別應用在可穿戴設備、收款方設備和伺服器上的電子支付裝置。這六種裝置均可以通過軟體實現，也可以通過硬體或者軟硬體結合的方式實現。以軟體實現為例，作為邏輯意義上的裝置，是通過可穿戴設備、終端、收款方設備或伺服器的 CPU（Central Process Unit，中央處理器）將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，除了圖 13 所示的 CPU、記憶體以及非易失性記憶體之外，裝置所在的可穿戴設備或終端通常還包括用於進行無線信號收發的晶片等其他硬體，裝置所在的收款方設備或伺服器通常還包括用

於實現網路通信功能的板卡等其他硬體。

圖 14 所示為本發明實施例提供的一種綁定可穿戴設備的裝置，應用在可穿戴設備上，包括設備資訊提供單元、設備憑證接收單元和設備憑證保存單元，其中：設備資訊提供單元用於向終端提供本設備的設備資訊；所述設備資訊包括設備標識，供終端向伺服器發送設備標識和使用終端的用戶帳戶；設備憑證接收單元用於接收來自伺服器的設備憑證，所述設備憑證由伺服器根據設備標識產生，並與所述用戶帳戶具有對應關係；設備憑證保存單元用於將設備憑證保存在本地，用來通過對應的用戶帳戶進行支付。

可選的，所述設備資訊提供單元具體用於：顯示攜帶有設備資訊的二維碼，供終端掃描。

可選的，所述設備憑證接收單元具體用於：接收終端轉發的來自伺服器的設備憑證。

可選的，所述裝置還包括授權請求發送單元，用於向伺服器發送授權請求，其中包括本設備的設備標識；所述設備憑證接收單元具體用於：接收伺服器發送的本設備的設備憑證。

可選的，所述設備憑證接收單元具體用於：接收來自伺服器的設備憑證和安全憑證，所述安全憑證用來在支付時對設備憑證進行校驗。

可選的，所述裝置還包括傳輸密鑰單元，用於產生用於在傳輸過程中加密設備憑證的設備端密鑰和服務端密

鑰，將設備端密鑰保存在本地，將服務端密鑰提供給伺服器；所述設備端密鑰與服務端密鑰相同或相對應；所述來自伺服器的設備憑證，包括：來自伺服器、經服務端密鑰加密後的設備憑證；所述裝置還包括傳輸解密單元，用於利用設備端密鑰解密接收的加密設備憑證，得到設備憑證。

可選的，所述設備憑證保存單元具體用於：將設備憑證採用加密演算法加密後，將密文保存在本地。

圖 15 所示為本發明實施例提供的一種綁定可穿戴設備的裝置，應用在伺服器上，包括綁定請求接收單元、設備憑證產生單元和設備憑證下發單元，其中：綁定請求接收單元用於接收終端發送的綁定請求；所述綁定請求中包括可穿戴設備的設備標識和使用終端的用戶帳戶；設備憑證產生單元用於根據設備標識產生可穿戴設備的設備憑證，保存設備憑證與所述用戶帳戶的對應關係；設備憑證下發單元用於將設備憑證提供給可穿戴設備，供可穿戴設備通過對應的用戶帳戶進行支付。

可選的，所述設備憑證下發單元具體用於：將設備憑證發送給終端，由終端轉發給可穿戴設備。

可選的，所述綁定請求中還包括：由可穿戴設備產生的服務端密鑰；所述設備憑證下發單元具體用於：以服務端密鑰對設備密鑰進行加密後發送給終端，由終端轉發給可穿戴設備。

可選的，所述裝置還包括：授權請求接收單元，用於

接收可穿戴設備發送的授權請求，其中包括可穿戴的設備標識；所述設備憑證下發單元具體用於：向可穿戴設備回覆對授權請求的回應，回應中包括設備憑證。

可選的，所述授權請求中還包括：由可穿戴設備產生的服務端密鑰；所述回應中包括的設備憑證為：經服務端密鑰加密後的設備憑證。

可選的，所述設備憑證下發單元具體用於：將設備憑證和安全憑證提供給可穿戴設備，所述安全憑證用來在支付時對設備憑證進行校驗。

圖 16 所示為本發明實施例提供的一種綁定可穿戴設備的裝置，應用在終端上，包括設備資訊獲取單元和綁定請求發送單元，其中：設備資訊獲取單元用於獲取可穿戴設備的設備資訊，其中包括可穿戴設備的設備標識；綁定請求發送單元用於向伺服器發送綁定請求；所述綁定請求中包括可穿戴設備的設備標識和使用本終端的用戶帳戶，供伺服器產生對應於用戶帳戶的設備憑證並提供給可穿戴設備；所述設備憑證由可穿戴設備用來通過對應的用戶帳戶進行支付。

可選的，所述裝置還包括設備憑證轉發單元，用於接收伺服器返回的設備憑證，並轉發給可穿戴設備。

可選的，所述裝置還包括傳輸密鑰接收單元，用於從可穿戴設備接收服務端密鑰；所述服務端密鑰由伺服器用來加密向可穿戴設備下發的設備憑證；所述綁定請求中還包括：服務端密鑰。

可選的，所述設備資訊獲取單元具體用於：掃描可穿戴設備顯示的二維碼，從二維碼資訊中得到可穿戴設備的設備資訊。

圖 17 所示為本發明實施例提供的一種電子支付裝置，應用在可穿戴設備上，所述可穿戴設備上保存有對應於用戶帳戶的設備憑證，所述裝置包括交易憑證產生單元和交易憑證提供單元，其中：交易憑證產生單元用於在收到用戶的指令後，根據保存的設備憑證產生交易憑證；交易憑證提供單元用於向收款方設備提供交易憑證，供收款方設備上傳到伺服器，在還原出設備憑證後以對應的用戶帳戶進行支付。

可選的，所述保存的設備憑證為採用加密演算法加密後的設備憑證密文；所述交易憑證產生單元具體用於：在收到用戶的指令後，讀取保存的設備憑證密文進行解密，根據解密後得到的設備憑證產生交易憑證。

可選的，所述可穿戴設備上還保存有對應於用戶帳戶的安全憑證；所述交易憑證產生單元具體用於：在收到用戶的指令後，根據保存的設備憑證和安全憑證，利用憑證產生演算法產生帶有校驗資訊的交易憑證；所述憑證產生演算法對應於伺服器根據交易憑證還原設備憑證和安全憑證所採用的憑證還原演算法。

可選的，所述交易憑證包括：二維碼或條碼。

圖 18 所示為本發明實施例提供的一種電子支付裝置，應用在伺服器上，所述伺服器可以獲得可穿戴設備的

設備憑證和使用所述可穿戴設備的用戶帳戶的對應關係，所述裝置包括收款請求接收單元、設備憑證還原單元和支付單元，其中：收款請求接收單元用於接收收款方設備發送的收款請求，收款請求中包括由可穿戴設備產生的交易憑證和款項資訊；設備憑證還原單元用於根據交易憑證還原所述可穿戴設備的設備憑證；支付單元用於按照款項資訊，以所述設備憑證對應的用戶帳戶作為支付方完成支付。

可選的，所述設備憑證還原單元具體用於：根據交易憑證，利用憑證還原演算法得到所述可穿戴設備的設備憑證和安全憑證；所述憑證還原演算法對應於可穿戴設備產生交易憑證所採用的憑證產生演算法；所述支付單元具體用於：利用安全憑證對交易憑證進行校驗，通過校驗後按照款項資訊，以所述設備憑證對應的用戶帳戶作為支付方完成支付。

可選的，所述裝置還包括支付結果發送單元，用於向收款方設備返回支付是否成功的結果。

圖 19 所示為本發明實施例提供的一種電子支付裝置，應用在收款方設備上，包括交易憑證獲取單元和收款請求發送單元，其中：交易憑證獲取單元用於獲取可穿戴設備的交易憑證；所述交易憑證由可穿戴設備根據其對應於用戶帳戶的設備憑證產生；收款請求發送單元用於向伺服器發送收款請求；收款請求中包括可穿戴設備的交易憑證和款項資訊，供伺服器由交易憑證還原出設備憑證，按

照款項資訊以對應於設備憑證的用戶帳戶進行支付。

可選的，所述裝置還包括支付結果接收單元，用於接收伺服器返回的支付是否成功的結果。

以上所述僅為本發明的較佳實施例而已，並不用以限制本發明，凡在本發明的精神和原則之內，所做的任何修改、等同替換、改進等，均應包含在本發明保護的範圍之內。

在一個典型的配置中，計算設備包括一個或多個處理器（CPU）、輸入/輸出介面、網路介面和記憶體。

記憶體可能包括電腦可讀媒體中的非永久性記憶體，隨機存取記憶體（RAM）和/或非易失性記憶體等形式，如唯讀記憶體（ROM）或快閃記憶體（flash RAM）。記憶體是電腦可讀媒體的示例。

電腦可讀媒體包括永久性和非永久性、可移動和非可移動媒體可以由任何方法或技術來實現資訊儲存。資訊可以是電腦可讀指令、資料結構、程式的模組或其他資料。電腦的儲存媒體的例子包括，但不限於相變記憶體（PRAM）、靜態隨機存取記憶體（SRAM）、動態隨機存取記憶體（DRAM）、其他類型的隨機存取記憶體（RAM）、唯讀記憶體（ROM）、電可擦除可編程唯讀記憶體（EEPROM）、快閃記憶體或其他記憶體技術、唯讀光碟唯讀記憶體（CD-ROM）、數位多功能光碟（DVD）或其他光學儲存、磁盒式磁帶，磁帶磁磁片儲存或其他磁性儲存設備或任何其他非傳輸媒體，可用於儲存

可以被計算設備存取的資訊。按照本文中的界定，電腦可讀媒體不包括暫存電腦可讀媒體（transitory media），如調變的資料信號和載波。

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儲存媒體（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。

I676945

發明摘要

※申請案號：105107433

※申請日：105 年 03 月 10 日

※IPC 分類：

【發明名稱】(中文/英文)

綁定可穿戴設備的方法和裝置、電子支付方法和裝置

【中文】

本發明提供一種綁定可穿戴設備的方法，應用在可穿戴設備上，包括：向終端提供本設備的設備資訊；所述設備資訊包括設備標識，供終端向伺服器發送設備標識和使用終端的用戶帳戶；接收來自伺服器的設備憑證，所述設備憑證由伺服器根據設備標識產生，並與所述用戶帳戶具有對應關係；將設備憑證保存在本地，用來通過對應的用戶帳戶進行支付。通過本發明的技術方案，即使在用戶使用的可穿戴設備與終端之間、或終端與伺服器之間的通信都斷開時，仍能通過可穿戴設備完成支付，提高了支付成功率，增加了用戶便利程度。

【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

申請專利範圍

1.一種綁定可穿戴設備的方法，應用在可穿戴設備上，其特徵在於，包括：

向終端提供本設備的設備資訊；該設備資訊包括設備標識，供終端向伺服器發送設備標識和使用終端的用戶帳戶；

接收來自伺服器的設備憑證，該設備憑證由伺服器根據設備標識產生，並與該用戶帳戶具有對應關係；

將設備憑證保存在本地，用來通過對應的用戶帳戶進行支付；

根據保存的設備憑證產生交易憑證；

根據交易憑證，利用憑證還原演算法得到該可穿戴設備的設備憑證和安全憑證；該憑證還原演算法對應於可穿戴設備產生交易憑證所採用的憑證產生演算法。

2.根據申請專利範圍第 1 項的方法，其中，該向終端提供本設備的設備資訊，包括：顯示攜帶有設備資訊的二維碼，供終端掃描。

3.根據申請專利範圍第 1 或 2 項的方法，其中，該接收來自伺服器的設備憑證，包括：接收終端轉發的來自伺服器的設備憑證。

4.根據申請專利範圍第 1 或 2 項的方法，其中，該方法還包括：向伺服器發送授權請求，其中包括本設備的設備標識；

該接收來自伺服器的設備憑證，包括：接收伺服器發

第 105107433 號

民國 108 年 6 月 19 日修正

送的本設備的設備憑證。

5.根據申請專利範圍第 1 項的方法，其中，該接收來自伺服器的設備憑證，包括：接收來自伺服器的設備憑證和安全憑證，該安全憑證用來在支付時對設備憑證進行校驗。

6.根據申請專利範圍第 1 項的方法，其中，該方法還包括：產生用於在傳輸過程中加密設備憑證的設備端密鑰和服務端密鑰，將設備端密鑰保存在本地，將服務端密鑰提供給伺服器；該設備端密鑰與服務端密鑰相同或相對應；

該來自伺服器的設備憑證，包括：來自伺服器、經服務端密鑰加密後的設備憑證；

該方法還包括：利用設備端密鑰解密接收的加密設備憑證，得到設備憑證。

7.根據申請專利範圍第 1 或 6 項的方法，其中，該將設備憑證保存在本地，包括：將設備憑證採用加密演算法加密後，將密文保存在本地。

8.一種綁定可穿戴設備的方法，應用在伺服器上，其特徵在於，包括：

接收終端發送的綁定請求；該綁定請求中包括可穿戴設備的設備標識和使用終端的用戶帳戶；

根據設備標識產生可穿戴設備的設備憑證，保存設備憑證與該用戶帳戶的對應關係；

將設備憑證提供給可穿戴設備，供可穿戴設備通過對

應的用戶帳戶進行支付；

根據可穿戴設備的設備憑證產生交易憑證；

根據交易憑證，利用憑證還原演算法得到該可穿戴設備的設備憑證和安全憑證；該憑證還原演算法對應於可穿戴設備產生交易憑證所採用的憑證產生演算法。

9.根據申請專利範圍第 8 項的方法，其中，該將設備憑證提供給可穿戴設備，包括：將設備憑證發送給終端，由終端轉發給可穿戴設備。

10.根據申請專利範圍第 9 項的方法，其中，該綁定請求中還包括：由可穿戴設備產生的服務端密鑰；

該將設備憑證提供給可穿戴設備，包括：以服務端密鑰對設備密鑰進行加密後發送給終端，由終端轉發給可穿戴設備。

11.根據申請專利範圍第 8 項的方法，其中，該方法還包括：接收可穿戴設備發送的授權請求，其中包括可穿戴的設備標識；

該將設備憑證提供給可穿戴設備，包括：向可穿戴設備回覆對授權請求的回應，回應中包括設備憑證。

12.根據申請專利範圍第 11 項的方法，其中，該授權請求中還包括：由可穿戴設備產生的服務端密鑰；

該回應中包括的設備憑證為：經服務端密鑰加密後的設備憑證。

13.根據申請專利範圍第 8 至 12 項中任一項的方法，其中，該將設備憑證提供給可穿戴設備，包括：將設備憑

第 105107433 號

民國 108 年 6 月 19 日修正

證和安全憑證提供給可穿戴設備，該安全憑證用來在支付時對設備憑證進行校驗。

14.一種綁定可穿戴設備的方法，應用在終端上，其特徵在於，包括：

獲取可穿戴設備的設備資訊，其中包括可穿戴設備的設備標識；

向伺服器發送綁定請求；該綁定請求中包括可穿戴設備的設備標識和使用本終端的用戶帳戶，供伺服器產生對應於用戶帳戶的設備憑證並提供給可穿戴設備；該設備憑證由可穿戴設備用來通過對應的用戶帳戶進行支付；

根據可穿戴設備的設備憑證產生交易憑證；

根據交易憑證，利用憑證還原演算法得到該可穿戴設備的設備憑證和安全憑證；該憑證還原演算法對應於可穿戴設備產生交易憑證所採用的憑證產生演算法。

15.根據申請專利範圍第 14 項的方法，其中，該方法還包括：接收伺服器返回的設備憑證，並轉發給可穿戴設備。

16.根據申請專利範圍第 14 項的方法，其中，該方法還包括：從可穿戴設備接收服務端密鑰；該服務端密鑰由伺服器用來加密向可穿戴設備下發的設備憑證；

該綁定請求中還包括：服務端密鑰。

17.根據申請專利範圍第 14 項的方法，其中，該獲取可穿戴設備的設備資訊，包括：掃描可穿戴設備顯示的二維碼，從二維碼資訊中得到可穿戴設備的設備資訊。

第 105107433 號

民國 108 年 6 月 19 日修正

18.一種電子支付方法，應用在可穿戴設備上，其特徵在於，該可穿戴設備上保存有對應於用戶帳戶的設備憑證，該方法包括：

收到用戶的指令後，根據保存的設備憑證產生交易憑證；

向收款方設備提供交易憑證，供收款方設備上傳到伺服器，在還原出設備憑證後以對應的用戶帳戶進行支付，

其中，該可穿戴設備上還保存有對應於用戶帳戶的安全憑證；該根據保存的設備憑證產生交易憑證，包括：根據保存的設備憑證和安全憑證，利用憑證產生演算法產生帶有校驗資訊的交易憑證；該憑證產生演算法對應於伺服器根據交易憑證還原設備憑證和安全憑證所採用的憑證還原演算法。

19.根據申請專利範圍第 18 項的方法，其中，該保存的設備憑證為採用加密演算法加密後的設備憑證密文；

該根據設備憑證產生交易憑證，包括：讀取保存的設備憑證密文進行解密，根據解密後得到的設備憑證產生交易憑證。

20.根據申請專利範圍第 18 項的方法，其中，該交易憑證包括：二維碼或條碼。

21.一種電子支付方法，應用在伺服器上，其特徵在於，該伺服器可以獲得可穿戴設備的設備憑證和使用該可穿戴設備的用戶帳戶的對應關係，該方法包括：

接收收款方設備發送的收款請求，收款請求中包括由

第 105107433 號

民國 108 年 6 月 19 日修正

可穿戴設備產生的交易憑證和款項資訊；

根據交易憑證還原該可穿戴設備的設備憑證；

按照款項資訊，以該設備憑證對應的用戶帳戶作為支付方完成支付，

其中，該根據交易憑證還原該可穿戴設備的設備憑證，包括：根據交易憑證，利用憑證還原演算法得到該可穿戴設備的設備憑證和安全憑證；該憑證還原演算法對應於可穿戴設備產生交易憑證所採用的憑證產生演算法。

22.根據申請專利範圍第 21 項的方法，其中，該按照款項資訊，以該設備憑證對應的用戶帳戶作為支付方完成支付，包括：利用安全憑證對交易憑證進行校驗，通過校驗後按照款項資訊，以該設備憑證對應的用戶帳戶作為支付方完成支付。

23.根據申請專利範圍第 21 項的方法，其中，該方法還包括：向收款方設備返回支付是否成功的結果。

24.一種電子支付方法，應用在收款方設備上，其特徵在於，包括：

獲取可穿戴設備的交易憑證；該交易憑證由可穿戴設備根據其對應於用戶帳戶的設備憑證產生；

向伺服器發送收款請求；收款請求中包括可穿戴設備的交易憑證和款項資訊，供伺服器由交易憑證還原出設備憑證，按照款項資訊以對應於設備憑證的用戶帳戶進行支付，

其中，該由交易憑證還原出設備憑證，包括：根據交

第 105107433 號

民國 108 年 6 月 19 日修正

易憑證，利用憑證還原演算法得到該可穿戴設備的設備憑證和安全憑證；該憑證還原演算法對應於可穿戴設備產生交易憑證所採用的憑證產生演算法。

25.根據申請專利範圍第 24 項的方法，其中，該方法還包括：接收伺服器返回的支付是否成功的結果。

26.一種綁定可穿戴設備的裝置，應用在可穿戴設備上，其特徵在於，包括：

設備資訊提供單元，用於向終端提供本設備的設備資訊；該設備資訊包括設備標識，供終端向伺服器發送設備標識和使用終端的用戶帳戶；

設備憑證接收單元，用於接收來自伺服器的設備憑證，該設備憑證由伺服器根據設備標識產生，並與該用戶帳戶具有對應關係；

設備憑證保存單元，用於將設備憑證保存在本地，用來通過對應的用戶帳戶進行支付；

設備憑證還原單元，用於根據保存的設備憑證產生交易憑證；根據交易憑證，利用憑證還原演算法得到該可穿戴設備的設備憑證和安全憑證；該憑證還原演算法對應於可穿戴設備產生交易憑證所採用的憑證產生演算法。

27.根據申請專利範圍第 26 項的裝置，其中，該設備資訊提供單元具體用於：顯示攜帶有設備資訊的二維碼，供終端掃描。

28.根據申請專利範圍第 26 或 27 項的裝置，其中，該設備憑證接收單元具體用於：接收終端轉發的來自伺服

第 105107433 號

民國 108 年 6 月 19 日修正

器的設備憑證。

29.根據申請專利範圍第 26 或 27 項的裝置，其中，該裝置還包括：授權請求發送單元，用於向伺服器發送授權請求，其中包括本設備的設備標識；

該設備憑證接收單元具體用於：接收伺服器發送的本設備的設備憑證。

30.根據申請專利範圍第 26 項的裝置，其中，該設備憑證接收單元具體用於：接收來自伺服器的設備憑證和安全憑證，該安全憑證用來在支付時對設備憑證進行校驗。

31.根據申請專利範圍第 26 項的裝置，其中，該裝置還包括：傳輸密鑰單元，用於產生用於在傳輸過程中加密設備憑證的設備端密鑰和服務端密鑰，將設備端密鑰保存在本地，將服務端密鑰提供給伺服器；該設備端密鑰與服務端密鑰相同或相對應；

該來自伺服器的設備憑證，包括：來自伺服器、經服務端密鑰加密後的設備憑證；

該裝置還包括：傳輸解密單元，用於利用設備端密鑰解密接收的加密設備憑證，得到設備憑證。

32.根據申請專利範圍第 26 或 31 項的裝置，其中，該設備憑證保存單元具體用於：將設備憑證採用加密演算法加密後，將密文保存在本地。

33.一種綁定可穿戴設備的裝置，應用在伺服器上，其特徵在於，包括：

綁定請求接收單元，用於接收終端發送的綁定請求；

第 105107433 號

民國 108 年 6 月 19 日修正

該綁定請求中包括可穿戴設備的設備標識和使用終端的用戶帳戶；

設備憑證產生單元，用於根據設備標識產生可穿戴設備的設備憑證，保存設備憑證與該用戶帳戶的對應關係；

設備憑證下發單元，用於將設備憑證提供給可穿戴設備，供可穿戴設備通過對應的用戶帳戶進行支付；

設備憑證還原單元，用於根據可穿戴設備的設備憑證產生交易憑證；根據交易憑證，利用憑證還原演算法得到該可穿戴設備的設備憑證和安全憑證；該憑證還原演算法對應於可穿戴設備產生交易憑證所採用的憑證產生演算法。

34.根據申請專利範圍第 33 項的裝置，其中，該設備憑證下發單元具體用於：將設備憑證發送給終端，由終端轉發給可穿戴設備。

35.根據申請專利範圍第 34 項的裝置，其中，該綁定請求中還包括：由可穿戴設備產生的服務端密鑰；

該設備憑證下發單元具體用於：以服務端密鑰對設備密鑰進行加密後發送給終端，由終端轉發給可穿戴設備。

36.根據申請專利範圍第 33 項的裝置，其中，該裝置還包括：授權請求接收單元，用於接收可穿戴設備發送的授權請求，其中包括可穿戴的設備標識；

該設備憑證下發單元具體用於：向可穿戴設備回覆對授權請求的回應，回應中包括設備憑證。

37.根據申請專利範圍第 36 項的裝置，其中，該授權

第 105107433 號

民國 108 年 6 月 19 日修正

請求中還包括：由可穿戴設備產生的服務端密鑰；

該回應中包括的設備憑證為：經服務端密鑰加密後的設備憑證。

38.根據申請專利範圍第 33 至 37 項中任一項的裝置，其中，該設備憑證下發單元具體用於：將設備憑證和安全憑證提供給可穿戴設備，該安全憑證用來在支付時對設備憑證進行校驗。

39.一種綁定可穿戴設備的裝置，應用在終端上，其特徵在於，包括：

設備資訊獲取單元，用於獲取可穿戴設備的設備資訊，其中包括可穿戴設備的設備標識；

綁定請求發送單元，用於向伺服器發送綁定請求；該綁定請求中包括可穿戴設備的設備標識和使用本終端的用戶帳戶，供伺服器產生對應於用戶帳戶的設備憑證並提供給可穿戴設備；該設備憑證由可穿戴設備用來通過對應的用戶帳戶進行支付；

設備憑證還原單元，用於根據可穿戴設備的設備憑證產生交易憑證；根據交易憑證，利用憑證還原演算法得到該可穿戴設備的設備憑證和安全憑證；該憑證還原演算法對應於可穿戴設備產生交易憑證所採用的憑證產生演算法。

40.根據申請專利範圍第 39 項的裝置，其中，該裝置還包括：設備憑證轉發單元，用於接收伺服器返回的設備憑證，並轉發給可穿戴設備。

第 105107433 號

民國 108 年 6 月 19 日修正

41.根據申請專利範圍第 39 項的裝置，其中，該裝置還包括：傳輸密鑰接收單元，用於從可穿戴設備接收服務端密鑰；該服務端密鑰由伺服器用來加密向可穿戴設備下發的設備憑證；

該綁定請求中還包括：服務端密鑰。

42.根據申請專利範圍第 39 項的裝置，其中，該設備資訊獲取單元具體用於：掃描可穿戴設備顯示的二維碼，從二維碼資訊中得到可穿戴設備的設備資訊。

43.一種電子支付裝置，應用在可穿戴設備上，其特徵在於，該可穿戴設備上保存有對應於用戶帳戶的設備憑證，該裝置包括：

交易憑證產生單元，用於在收到用戶的指令後，根據保存的設備憑證產生交易憑證；

交易憑證提供單元，用於向收款方設備提供交易憑證，供收款方設備上傳到伺服器，在還原出設備憑證後以對應的用戶帳戶進行支付，

其中，該可穿戴設備上還保存有對應於用戶帳戶的安全憑證；該交易憑證產生單元具體用於：在收到用戶的指令後，根據保存的設備憑證和安全憑證，利用憑證產生演算法產生帶有校驗資訊的交易憑證；該憑證產生演算法對應於伺服器根據交易憑證還原設備憑證和安全憑證所採用的憑證還原演算法。

44.根據申請專利範圍第 43 項的裝置，其中，該保存的設備憑證為採用加密演算法加密後的設備憑證密文；

第 105107433 號

民國 108 年 6 月 19 日修正

該交易憑證產生單元具體用於：在收到用戶的指令後，讀取保存的設備憑證密文進行解密，根據解密後得到的設備憑證產生交易憑證。

45.根據申請專利範圍第 45 項的裝置，其中，該交易憑證包括：二維碼或條碼。

46.一種電子支付裝置，應用在伺服器上，其特徵在於，該伺服器可以獲得可穿戴設備的設備憑證和使用該可穿戴設備的用戶帳戶的對應關係，該裝置包括：

收款請求接收單元，用於接收收款方設備發送的收款請求，收款請求中包括由可穿戴設備產生的交易憑證和款項資訊；

設備憑證還原單元，用於根據交易憑證還原該可穿戴設備的設備憑證；

支付單元，用於按照款項資訊，以該設備憑證對應的用戶帳戶作為支付方完成支付，

其中，該設備憑證還原單元具體用於：根據交易憑證，利用憑證還原演算法得到該可穿戴設備的設備憑證和安全憑證；該憑證還原演算法對應於可穿戴設備產生交易憑證所採用的憑證產生演算法。

47.根據申請專利範圍第 46 項的裝置，其中，該支付單元具體用於：利用安全憑證對交易憑證進行校驗，通過校驗後按照款項資訊，以該設備憑證對應的用戶帳戶作為支付方完成支付。

48.根據申請專利範圍第 46 項的裝置，其中，該裝置

第 105107433 號

民國 108 年 6 月 19 日修正

還包括：支付結果發送單元，用於向收款方設備返回支付是否成功的結果。

49.一種電子支付裝置，應用在收款方設備上，其特徵在於，包括：

交易憑證獲取單元，用於獲取可穿戴設備的交易憑證；該交易憑證由可穿戴設備根據其對應於用戶帳戶的設備憑證產生；

收款請求發送單元，用於向伺服器發送收款請求；收款請求中包括可穿戴設備的交易憑證和款項資訊，供伺服器由交易憑證還原出設備憑證，按照款項資訊以對應於設備憑證的用戶帳戶進行支付，

其中，該由交易憑證還原出設備憑證，包括：根據交易憑證，利用憑證還原演算法得到該可穿戴設備的設備憑證和安全憑證；該憑證還原演算法對應於可穿戴設備產生交易憑證所採用的憑證產生演算法。

50.根據申請專利範圍第 49 項的裝置，其中，該裝置還包括：支付結果接收單元，用於接收伺服器返回的支付是否成功的結果。