201730826

(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 201730826 A

(43)公開日： 中華民國 106 (2017) 年 09 月 01 日

(21)申請案號：105143647 (22)申請日： 中華民國 105 (2016) 年 12 月 28 日

(51)Int. Cl.： *G06Q20/40 (2012.01)* *G06Q20/34 (2012.01)*
H04L9/30 (2006.01)

(30)優先權：2016/01/25 中國大陸 201610051643.8

(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：陳星 (CN) ；王磊 (CN) ；沈悅斌 (CN)

(74)代理人：林志剛

申請實體審查：無 申請專利範圍項數：18 項 圖式數：25 共 63 頁

(54)名稱

基於移動終端卡模擬的信用支付方法及裝置

(57)摘要

本發明是關於一種基於移動終端卡模擬的信用支付方法及裝置，其方法包括：向預設伺服器發送應用授權請求；接收預設伺服器發送的應用公鑰證書和應用私鑰；將應用公鑰證書和應用私鑰保存到移動終端的信用支付應用中；向預設伺服器發送信用支付資料獲取請求；接收預設伺服器發送的信用支付資料，並根據信用支付資料開通所述移動終端的信用支付功能。當用戶開通支付應用之後，可以透過使用移動終端就可以完成對交易終端的離線信用支付，可以快速、安全的完成支付交易，並且無需線上支付，避免了相關技術中，例如用戶在乘坐公共交通工具時，還需要用戶使用現金或公交卡等方式才能實現支付交易功能。

指定代表圖：

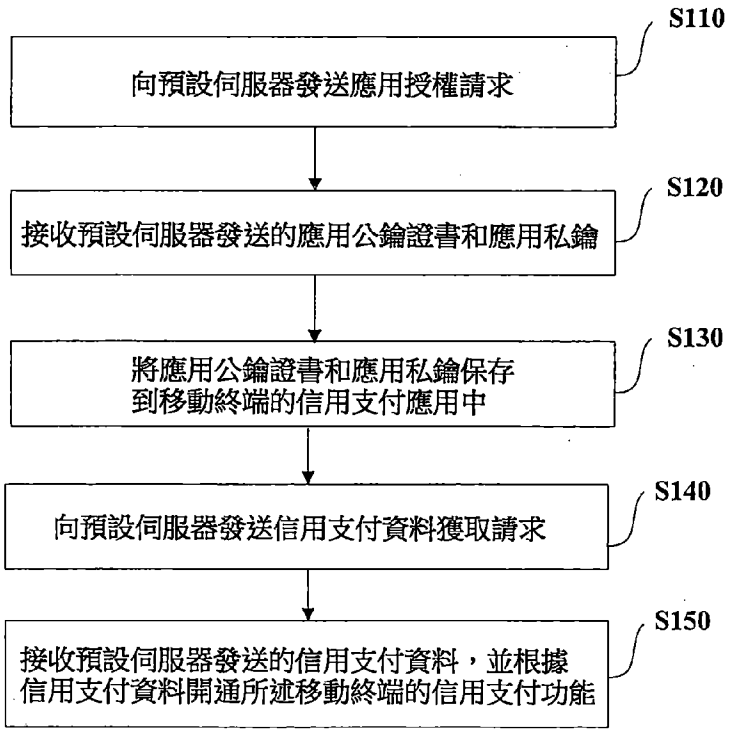
S110
向預設伺服器發送應用授權請求
S120
接收預設伺服器發送的應用公鑰證書和應用私鑰
S130
將應用公鑰證書和應用私鑰保存
到移動終端的信用支付應用中
S140
向預設伺服器發送信用支付資料獲取請求
S150
接收預設伺服器發送的信用支付資料，並根據
信用支付資料開通所述移動終端的信用支付功能

圖 2

201730826

發明摘要

※申請案號：105143647

※申請日：105 年 12 月 28 日　　※IPC 分類：G06Q 20/40 (2012.01)
G06Q 20/34 (2012.01)
H04L 9/30 (2006.01)

【發明名稱】(中文/英文)

基於移動終端卡模擬的信用支付方法及裝置

【中文】

本發明是關於一種基於移動終端卡模擬的信用支付方法及裝置，其方法包括：向預設伺服器發送應用授權請求；接收預設伺服器發送的應用公鑰證書和應用私鑰；將應用公鑰證書和應用私鑰保存到移動終端的信用支付應用中；向預設伺服器發送信用支付資料獲取請求；接收預設伺服器發送的信用支付資料，並根據信用支付資料開通所述移動終端的信用支付功能。當用戶開通支付應用之後，可以透過使用移動終端就可以完成對交易終端的離線信用支付，可以快速、安全的完成支付交易，並且無需線上支付，避免了相關技術中，例如用戶在乘坐公共交通工具時，還需要用戶使用現金或公交卡等方式才能實現支付交易功能。

【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

(本申請書格式、順序，請勿任意更動)

【發明名稱】(中文/英文)

基於移動終端卡模擬的信用支付方法及裝置

【技術領域】

本發明係關於通信技術領域，尤其關於一種基於移動終端卡模擬的信用支付方法及裝置。

【先前技術】

目前公共交通工具主要包括公交和地鐵，而用戶在乘坐公共交通工具購票時，主要採用現金或公交卡兩種支付方式，現金支付主要針對公交系統，用戶可以採用投幣的形式購票。同時，用戶也可以採用預付費的方式辦理公交卡，以刷卡的形式乘坐公車或地鐵出行。

用戶在使用現金的方式購票乘坐公車時，一方面，由於很多公車為無人售票車，不設找兌，使得用戶須事先準備小額票款，給用戶出行帶來了不便。另一方面，公交系統的工作人員在營業結束後，還需對用戶在乘坐無人售票公車時投入的小額票款清點，給工作人員帶來了額外的工作。用戶在使用公交卡刷卡乘坐公共交通工具時，由於目前公交卡主要為非接觸式射頻卡，用戶在使用和攜帶過程中，容易造成公交卡的彎折損壞、卡面的磨損致使卡面圖案模糊等人為損耗。當用戶乘坐公共交通工具使用單次公

交卡時，也大多使用小額票款購買單次公交卡，同樣需要工作人員對小額票款進行清點結算。

當用戶乘坐公共交通工具使用可複用的預付費公交卡時，由於該可複用的預付費公交卡不記名、不掛失，丟失後會給用戶造成很大的損失，並且還需要用戶去指定的網點購買、充值和退款，同樣給用戶造成很大不便。

【發明內容】

為克服相關技術中存在的問題，本發明提供一種基於移動終端卡模擬的信用支付方法及裝置。

根據本發明實施例的第一態樣，提供一種基於移動終端卡模擬的信用支付方法，包括：

向預設伺服器發送應用授權請求；

接收所述預設伺服器發送的應用公鑰證書和應用私鑰；

將所述應用公鑰證書和所述應用私鑰保存到所述移動終端的信用支付應用中；

向所述預設伺服器發送信用支付資料獲取請求；

接收所述預設伺服器發送的信用支付資料，並根據所述信用支付資料開通所述移動終端的信用支付功能。

進一步的，還包括：

獲取所述移動終端的設備參數資訊；

將所述設備參數資訊發送給所述預設伺服器，以使所述預設伺服器根據接收到的所述設備參數資訊判斷所述移

動終端是否滿足開通信用支付的硬體條件；

檢測是否接收到所述預設伺服器發送的信用支付開通資訊；

當接收到所述預設伺服器發送的信用支付開通資訊時，確定所述移動終端滿足開通信用支付的硬體條件，並執行所述向預設伺服器發送應用授權請求的步驟。

進一步的，還包括：

獲取用戶身份資訊；

將所述用戶身份資訊發送給所述預設伺服器，以使所述預設終端根據接收到的所述用戶身份資訊判斷所述移動終端是否滿足開通信用支付的安全認證條件；

檢測是否接收到所述預設伺服器發送的安全認證通過資訊；

當接收到所述預設伺服器發送的安全認證通過資訊時，確定所述移動終端滿足開通信用支付的安全認證條件，並執行所述向預設伺服器發送應用授權請求的步驟。

進一步的，還包括：

向所述預設伺服器發送獲取預設安裝檔的請求；所述預設安裝檔包括：信用支付安裝檔；

獲取所述預設伺服器發送的所述預設安裝檔；

將所述預設安裝檔安裝在所述移動終端中，執行所述向預設伺服器發送應用授權請求的步驟。

進一步的，所述信用支付資料，包括：支付卡號、信用額度、可用額度和交易驗證碼 TAC 子密鑰。

根據本發明實施例的第二態樣，提供一種基於移動終端卡模擬的信用支付方法，包括：

接收移動終端發送的應用授權請求；

根據所述應用授權請求分別生成應用公鑰和應用私鑰；

利用所述預設伺服器中保存的信用授權私鑰對所述應用公鑰簽名，生成應用公鑰證書；

將所述應用公鑰證書和所述應用私鑰發送給所述移動終端；

接收所述移動終端發送的信用支付資料獲取請求；

根據所述信用支付資料獲取請求，生成與所述移動終端相對應信用支付資料，並將所述信用支付資料發送給所述移動終端，以使所述移動終端根據接收到的信用支付資料開通所述移動終端的信用支付功能。

進一步的，還包括：

接收所述移動終端發送的設備參數資訊；

根據所述設備參數資訊判斷所述移動終端是否滿足開通信用支付的硬體條件；

當所述移動終端滿足開通信用支付的硬體條件時，向所述移動終端發送信用支付開通資訊，並執行所述接收移動終端發送的應用授權請求的步驟。

進一步的，還包括：

接收所述移動終端發送的用戶身份資訊；

根據所述用戶身份資訊判斷所述移動終端是否滿足開

通信用支付的安全認證條件；

當所述身份資訊滿足開通信用支付的安全認證條件時，向所述移動終端發送安全認證通過資訊，並執行所述接收移動終端發送的應用授權請求的步驟。

進一步的，還包括：

接收所述移動終端發送的獲取預設安裝檔的請求，所述預設安裝檔包括：信用支付安裝檔；

根據所述獲取預設安裝檔的請求將所述預設安裝檔發送給所述移動終端，並執行所述接收移動終端發送的應用授權請求的步驟。

根據本發明實施例的第三態樣，提供一種基於移動終端卡模擬的信用支付裝置，包括：

應用授權請求發送單元，用於利用所述移動終端中的信用授權系統應用向預設伺服器發送應用授權請求；

密鑰接收單元，用於接收所述預設伺服器發送的應用公鑰證書和應用私鑰；

密鑰保存單元，用於將所述應用公鑰證書和所述應用私鑰保存到所述移動終端的信用支付應用中；

信用支付資料獲取請求發送單元，用於向所述預設伺服器發送信用支付資料獲取請求；

信用支付資料接收單元，用於接收所述預設伺服器發送的信用支付資料；

信用支付完成單元，用於根據所述信用支付資料開通所述移動終端的信用支付功能。

進一步的，還包括：

設備參數資訊獲取單元，用於獲取所述移動終端的設備參數資訊；

設備參數資訊發送單元，用於將所述設備參數資訊發送給所述預設伺服器，以使所述預設伺服器根據接收到的所述設備參數資訊判斷所述移動終端是否滿足開通信用支付的硬體條件；

第一檢測單元，用於檢測是否接收到所述預設伺服器發送的信用支付開通資訊；

硬體條件確定單元，用於在接收到所述預設伺服器發送的信用支付開通資訊時，確定所述移動終端滿足開通信用支付的硬體條件。

進一步的，還包括：

用戶身份資訊獲取單元，用於獲取用戶身份資訊；

用戶身份資訊發送單元，用於將所述用戶身份資訊發送給所述預設伺服器，以使所述預設終端根據接收到的所述用戶身份資訊判斷所述移動終端是否滿足開通信用支付的安全認證條件；

第二檢測單元，用於檢測是否接收到所述預設伺服器發送的安全認證通過資訊；

安全認證條件確定單元，用於在接收到所述預設伺服器發送的安全認證通過資訊時，確定所述移動終端滿足開通信用支付的安全認證條件。

進一步的，還包括：

獲取預設安裝檔請求發送單元，用於向所述預設伺服器發送獲取預設安裝檔的請求；所述預設安裝檔包括：信用支付安裝檔；

預設安裝檔獲取單元，用於獲取所述預設伺服器發送的所述預設安裝檔；

安裝單元，用於將所述預設安裝檔安裝在所述移動終端中。

進一步的，所述信用支付資料，包括：支付卡號、信用額度、可用額度和交易驗證碼 TAC 子密鑰。

根據本發明實施例的第四態樣，提供一種基於移動終端卡模擬的信用支付裝置，包括：

應用授權請求接收單元，用於接收移動終端發送的應用授權請求；

密鑰生成單元，用於根據所述應用授權請求分別生成應用公鑰和應用私鑰；

應用公鑰證書生成單元，用於利用所述預設伺服器中保存的信用授權私鑰對所述應用公鑰簽名，生成應用公鑰證書；

資料發送單元，用於將所述應用公鑰證書和所述應用私鑰發送給所述移動終端；

信用支付資料獲取請求接收單元，用於接收所述移動終端發送的信用支付資料獲取請求；

信用支付資料生成單元，用於根據所述信用支付資料獲取請求，生成與所述移動終端相對應信用支付資料；

信用支付資料發送單元，用於將所述信用支付資料發送給所述移動終端，以使所述移動終端根據接收到的信用支付資料開通所述移動終端的信用支付功能。

進一步的，還包括：

設備參數資訊接收單元，用於接收所述移動終端發送的設備參數資訊；

第一判斷單元，用於根據所述設備參數資訊判斷所述移動終端是否滿足開通信用支付的硬體條件；

信用支付開通資訊發送單元，用於在所述移動終端滿足開通信用支付的硬體條件時，向所述移動終端發送信用支付開通資訊。

進一步的，還包括：

用戶身份資訊接收單元，用於接收所述移動終端發送的用戶身份資訊；

第二判斷單元，用於根據所述用戶身份資訊判斷所述移動終端是否滿足開通信用支付的安全認證條件；

安全認證通過資訊發送單元，用於在所述身份資訊滿足開通信用支付的安全認證條件時，向所述移動終端發送安全認證通過資訊。

進一步的，還包括：

預設安裝檔請求接收單元，用於接收所述移動終端發送的獲取預設安裝檔的請求，所述預設安裝檔包括：信用支付安裝檔；

預設安裝檔發送單元，用於根據所述獲取預設安裝檔

的請求將所述預設安裝檔發送給所述移動終端。

本發明的實施例提供的技術方案可以包括以下有益效果：

本發明提供的基於移動終端卡模擬的信用支付方法及裝置，可以應用在移動終端和交易終端中，當用戶開通支付應用之後，可以透過使用移動終端就可以完成對交易終端的離線信用支付，可以快速、安全的完成支付交易，並且無需線上支付，避免了相關技術中，例如用戶在乘坐公共交通工具時，還需要用戶使用現金或公交卡等方式才能實現支付交易功能。

應當理解的是，以上的一般描述和後文的細節描述僅是示例性和解釋性的，並不能限制本發明。

【圖式簡單說明】

此處的附圖被併入說明書中並構成本說明書的一部分，示出了符合本發明的實施例，並與說明書一起用於解釋本發明的原理。

圖 1 是發明實施例中提供的信用授權系統示意圖；

圖 2 是根據一示例性實施例示出的一種基於移動終端卡模擬的信用支付方法流程圖；

圖 3 是根據另一示例性實施例示出的一種基於移動終端卡模擬的信用支付方法流程圖；

圖 4 是根據又一示例性實施例示出的一種基於移動終端卡模擬的信用支付方法流程圖；

圖 5 是根據又一示例性實施例示出的一種基於移動終端卡模擬的信用支付方法流程圖；

圖 6 是根據又一示例性實施例示出的一種基於移動終端卡模擬的信用支付方法流程圖；

圖 7 是根據又一示例性實施例示出的一種基於移動終端卡模擬的信用支付方法流程圖；

圖 8 是根據又一示例性實施例示出的一種基於移動終端卡模擬的信用支付方法流程圖；

圖 9 是根據又一示例性實施例示出的一種基於移動終端卡模擬的信用支付方法流程圖；

圖 10 是根據又一示例性實施例示出的一種基於移動終端卡模擬的信用支付方法流程圖；

圖 11 是圖 10 中步驟 150 的流程圖；

圖 12 是根據又一示例性實施例示出的一種基於移動終端卡模擬的信用支付方法流程圖；

圖 13 是圖 12 中步驟 460 的流程圖；

圖 14 是根據又一示例性實施例示出的一種基於移動終端卡模擬的信用支付方法流程圖；

圖 15 是信用授權系統應用、信用支付應用及信用授權系統的服務端之間信令圖；

圖 16 是移動終端與公交閘機之間的資料交互的信令圖；

圖 17 是公交閘機與信用授權系統的服務端之間的資料交互流的信令圖；

圖 18 是根據一示例性實施例示出的一種基於移動終端卡模擬的信用支付裝置示意圖；

圖 19 是根據又一示例性實施例示出的一種基於移動終端卡模擬的信用支付裝置示意圖；

圖 20 是根據又一示例性實施例示出的一種基於移動終端卡模擬的信用支付裝置示意圖；

圖 21 是根據又一示例性實施例示出的一種基於移動終端卡模擬的信用支付裝置示意圖；

圖 22 是根據又一示例性實施例示出的一種基於移動終端卡模擬的信用支付裝置示意圖；

圖 23 是根據又一示例性實施例示出的一種基於移動終端卡模擬的信用支付裝置示意圖；

圖 24 是根據又一示例性實施例示出的一種基於移動終端卡模擬的信用支付裝置示意圖；

圖 25 是根據又一示例性實施例示出的一種基於移動終端卡模擬的信用支付裝置示意圖。

【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發明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、本發明的一些方態樣一致的裝置和方法的例子。

移動支付(Mobile Payment)，也稱手機支付，用戶可以使用移動終端對所購買的商品或者服務進行帳務支付。移動終端可以採用 NFC（Near Field Communication，近場通信）與交易終端通信，實現支付交易。其中，NFC 又稱近距離通信，是一種短距離的高頻無線通訊技術，允許電子設備之間進行非接觸式點對點資料傳輸交換資料。由於近場通信具有天然的安全性，因此，NFC 技術在支付等領域具有很大的應用前景。

卡模擬是 NFC 技術的三種工作模式之一，這個卡模擬其實就是相當於一張採用 RFID（Radio Frequency Identification，射頻識別）技術的 IC（integrated circuit，積體電路）卡，可以替代大量的 IC 卡(包括信用卡)使用的場合，如商場刷卡、公交卡、門禁管制，車票，門票等等。此種方式下，有一個極大的優點，那就是卡片透過非接觸讀卡器的 RF 域來供電，即使寄主設備(如手機)沒電也可以工作。

為了便於本領域技術人員理解和實施本發明，首先簡要說明本發明實施例中涉及到的移動終端、支付終端及伺服器之間的相互關係，如上述各終端之間的資料如何傳輸和處理等。由於本發明可以用在包括移動支付在內的很多領域，為了便於說明，本發明實施例中以用戶乘坐公共交通工具時，透過刷手機進行信用支付為例進行說明。

如圖 1 所示，本發明實施例中提供的信用授權系統應用包括：移動終端 100、交易終端 200 和伺服器 300。其

中，移動終端 100 可以是帶有支付交易功能的手機；交易終端 200 可以是公交閘機，公交閘機是指公交、地鐵系統中使用的 POS 機；伺服器 300 是信用授權系統應用的服務端。在用戶透過移動終端 100 與交易終端 200 進行支付交易之前，還需要透過伺服器 300 開通移動終端 100 的信用支付交易功能，然後才能實現移動終端 100 與交易終端 200 的支付交易。並且交易終端 200 會定期上傳移動終端 100 的交易日誌給伺服器 300，伺服器 300 會對移動終端 100 對應的帳戶內扣除相應的金額，並將該金額支付給公交公司。

在本發明提供的實施例中，移動終端中可安裝有兩個應用，一個是信用支付應用，例如信用支付應用 Applet，該應用 Applet 對於 Java 卡來講，Sun 公司定了 Applet 作為其上運行的 Applet 的對象。移動終端上的另一應用可以是信用授權系統應用。可以理解，該兩個應用的功能也可以是同一個應用來實現。

交易終端 200 會使用嚴格的身份安全認證機制，保證只有身份通過安全認證，而且有足夠信用額度的用戶才能開通公交信用支付應用。

信用支付應用 Applet 安裝在具有 NFC 功能移動終端 100 中，在個人化時生成應用公私密鑰對，並將應用私鑰保存在信用支付應用中，由信用支付應用保證其資料在任何條件下均不可被盜取，應用公鑰由信用授權系統應用的私鑰簽發成應用公鑰證書，保存到信用支付應用中。信用

授權系統應用的公鑰會提供給交易終端 200，保存位置由交易終端 200 決定，由於其為公鑰，所以對安全方面可以不需要強制性的要求。

提供信用支付交易時，交易終端 200 在讀取到信用支付應用中的應用公鑰證書以後，使用信用授權系統應用的公鑰驗簽，恢復出應用公鑰。信用支付應用會使用應用私鑰生成支付授權許可，交易終端 200 使用應用公鑰對支付授權許可進行驗簽，通過後再對授權許可中的安全因數進行檢查，確認安全後進行信用記帳，隨後在指定時間再向相應的信用帳戶進行結算。為了保證安全，當使用次數，額度和間隔時間任一因素超過指定閾值，均需要移動終端聯網對用戶的身份資訊進行驗證，需重新授權，確保信用支付的安全性。

為了解決相關技術問題，本發明實施例首先提供了一種基於移動終端卡模擬的信用支付方法，用於在移動終端開通信用支付的過程中，如圖 2 所示，該方法可以包括如下步驟：

在步驟 S110 中，向預設伺服器發送應用授權請求。

信用授權系統應用安裝在移動終端中，移動終端可以透過授權系統應用向信用授權系統的服務端發送應用授權請求。

在步驟 S120 中，接收預設伺服器發送的應用公鑰證書和應用私鑰。

信用授權系統的服務端根據接收到的應用授權請求，

生成一對應用公私鑰，即應用公鑰和應用私鑰，服務端利用本地儲存的授權私鑰對應用公鑰簽名，生成應用公鑰證書，將得到的應用公鑰證書和應用私鑰分別發送給移動終端。

在步驟 S130 中，將應用公鑰證書和應用私鑰保存到移動終端的信用支付應用中。

移動終端將服務端發送的應用公鑰證書及應用私鑰保存到移動終端的信用支付應用中。

在步驟 S140 中，向預設伺服器發送信用支付資料獲取請求。

在步驟 S150 中，接收預設伺服器發送的信用支付資料，並根據信用支付資料開通所述移動終端的信用支付功能。

信用支付資料可以是個人化腳本，其中，個人化腳本可包括：支付卡號、信用額度、可用額度、TAC 子密鑰。其中，支付卡號是信用授權系統為每一個用戶的信用支付應用生成的唯一特徵碼。可用額度是用戶當前可以使用的金額。並且 TAC 子密鑰是信用授權系統服務端使用 TAC 母密鑰根據卡號散列得到的。

在本發明提供的又一實施例中，基於圖 2，如圖 3 所示，在步驟 S110 之前，還可以包括如下步驟：

在步驟 S101 中，獲取移動終端的設備參數資訊。

移動終端的設備參數資訊可以是移動終端的硬體資訊，需要根據該設備參數資訊檢測該移動終端是否具備支

付交易所具備的硬體條件，如是否具有 NFC 功能等。當然，設備參數資訊還可以是移動終端的設備型號、ROM 版本、系統型號（如 android 版本）和應用版本等資訊。

在步驟 S102 中，將設備參數資訊發送給預設伺服器。

移動終端將獲取到自身的設備參數資訊發送給信用授權系統的服務端，以使服務端根據接收到的設備參數資訊判斷該移動終端是否滿足開通信用支付的硬體條件。

在步驟 S103 中，檢測是否接收到預設伺服器發送的信用支付開通資訊。

如果移動終端滿足開通信用支付的硬體條件，那麼服務端會向移動終端發送信用支付開通資訊。其中，該信用支付開通資訊可以是信用支付應用開通頁面。

如果移動終端不滿足開通信用支付的硬體條件，那麼服務端不會向移動終端發送信用支付開通資訊。

當接收到預設伺服器發送的信用支付開通資訊時，執行步驟 S104。

在步驟 S104 中，確定移動終端滿足開通信用支付的硬體條件，隨後執行步驟 S110。

除了需要檢測移動終端是否滿足開通信用支付的硬體條件，基於圖 2，在步驟 S110 之前，如圖 4 所示，還需要檢測移動終端是否滿足安全認證條件，因此，在本發明提供的又一實施例中，本發明提供的基於移動終端卡模擬的信用支付方法，還可以包括以下步驟：

在步驟 S105 中，獲取用戶身份資訊。

用戶的身份資訊，可以是用戶的身份證號碼、姓名、銀行卡號、郵箱及支付寶帳號等資訊。

在步驟 S106 中，將用戶身份資訊發送給預設伺服器。以使預設終端根據接收到的用戶身份資訊判斷移動終端是否滿足開通信用支付的安全認證條件。

移動終端將用戶身份資訊發送給信用授權系統的服務端，以使服務端對用戶身份資訊進行驗證，如驗證銀行卡號是否正常提供服務，該用戶帳號是否有信用不良交易記錄等。

在步驟 S107 中，檢測是否接收到預設伺服器發送的安全認證通過資訊。

服務端在接收到移動終端發送的用戶資訊之後，會對該用戶資訊進行檢查，如果滿足開通信用支付的安全認證條件，那麼會向移動終端發送安全認證通過資訊。

當接收到預設伺服器發送的安全認證通過資訊時，在步驟 S108 中，確定移動終端滿足開通信用支付的安全認證條件，隨後執行步驟 S110。

當移動終端接收到服務端發送的安全認證通過資訊時，確定移動終端滿足開通信用支付的安全認證條件。

當移動終端沒有接收到服務端發送的安全認證通過資訊時，確定移動終端不滿足開通信用支付的安全認證條件。

基於圖 2，在步驟 S110 之前，如圖 5 所示，還需要

在移動終端安裝相關應用，因此，本發明提供的基於移動終端卡模擬的信用支付方法，還包括如下步驟：

在步驟 S160 中，向預設伺服器發送獲取預設安裝檔的請求。

預設安裝檔包括：信用支付安裝應用。

在步驟 S170 中，獲取預設伺服器發送的預設安裝檔。

在步驟 S180 中，將預設安裝檔安裝在移動終端中。隨後執行步驟 S110。

將信用支付應用和註冊腳本分別安裝移動終端後，相當於移動終端的用戶個人化完成。那麼移動終端側開通信用支付功能的流程結束，結合上述實施例，下面對移動終端開通信用支付功能的信用授權系統的服務端側的執行流程做出詳細闡述。

在本發明提供的又一實施例中，如圖 6 所示，本發明提供的基於移動終端卡模擬的信用支付方法，在伺服器（信用授權系統的服務端）的執行流程，可以包括以下步驟：

在步驟 S210 中，接收移動終端發送的應用授權請求。

在步驟 S220 中，根據應用授權請求分別生成應用公鑰和應用私鑰。

在步驟 S230 中，利用預設伺服器中保存的信用授權私鑰對應用公鑰簽名，生成應用公鑰證書。

在步驟 S240 中，將應用公鑰證書和應用私鑰發送給移動終端。

信用授權系統的服務端根據接收到的應用授權請求，生成一對應用公私鑰，即應用公鑰和應用私鑰，服務端利用本地儲存的授權私鑰對應用公鑰簽名，生成應用公鑰證書，將得到的應用公鑰證書和應用私鑰分別發送給移動終端。

在步驟 S250 中，接收移動終端發送的信用支付資料獲取請求。

在步驟 S260 中，根據信用支付資料獲取請求，生成與移動終端相對應信用支付資料，並將信用支付資料發送給移動終端，以使移動終端根據接收到的信用支付資料開通所述移動終端的信用支付功能。

信用支付資料可以是個人化腳本，其中，個人化腳本包括：支付卡號、信用額度、可用額度、TAC 子密鑰。其中，支付卡號是信用授權系統為每一個用戶的信用支付應用生成的唯一特徵碼。可用額度是用戶當前可以使用的金額。並且 TAC 子密鑰是信用授權系統服務端使用 TAC 母密鑰根據卡號散列得到的。

基於圖 6，如圖 7 所示，在本發明提供的又一實施例中，伺服器（信用授權系統的服務端）根據移動終端發送的設備參數資訊，判斷該移動終端是否滿足開通信用支付的硬體條件，因此，本發明實施例中提供的基於移動終端卡模擬的信用支付方法，在步驟 S210 之前，還可以包括

以下步驟：

在步驟 S201 中，接收移動終端發送的設備參數資訊。

在移動終端開通信用支付功能的過程中，可以透過網路等方式與信用授權系統的服務端（即伺服器）通信，信用授權系統的服務端可以接收移動終端發送的設備參數資訊。

在步驟 S202 中，根據設備參數資訊判斷移動終端是否滿足開通信用支付的硬體條件。

移動終端發送的參數資訊，可以是移動終端的設備型號、ROM 版本、系統型號（如 android 版本）和應用版本等資訊等。服務端可以根據移動終端發送的上述資訊檢測移動終端是否有具備 NFC 功能等。

如果服務端檢測到移動終端滿足開通信用支付的硬體條件，那麼服務端會向移動終端發送信用支付開通資訊。其中，該信用支付開通資訊可以是信用支付應用開通頁面。用戶可以在移動終端上的信用支付應用開通介面上輸入用戶資訊上傳到服務端。

如果服務端檢測到移動終端不滿足開通信用支付的硬體條件，那麼服務端不會向移動終端發送信用支付開通資訊。

當移動終端滿足開通信用支付的硬體條件時，在步驟 S203 中，向移動終端發送信用支付開通資訊。隨後執行步驟 S210。

信用授權系統的服務端除了要檢測移動終端發送的設備參數資訊，還需要檢測移動終端發送的用戶身份資訊，判斷移動終端對應的用戶是否滿足安全認證條件。因此，基於圖 6，如圖 8 所示，本發明提供的基於移動終端卡模擬的信用支付方法，在移動終端開通信用支付功能的過程中，在步驟 S210 之前，還可以包括如下步驟：

在步驟 S204 中，接收移動終端發送的用戶身份資訊。

該用戶身份資訊可以是用戶的身份證號碼、姓名、銀行卡號、郵箱及支付寶帳號等資訊。

在步驟 S205 中，根據用戶身份資訊判斷移動終端是否滿足開通信用支付的安全認證條件。

示例性的，服務端可以檢測用戶身份資訊中的一銀行卡號是否正常提供服務，是否有不良交易記錄等。

如果服務端檢測到移動終端滿足開通信用支付的安全認證條件，那麼會向移動終端發送安全認證通過資訊。

當身份資訊滿足開通信用支付的安全認證條件時，在步驟 S206 中，向移動終端發送安全認證通過資訊。隨後執行步驟 S210。

移動終端在開通信用支付時，還需要安裝信用支付應用，而這些安裝檔都需要信用支付系統的服務端發送給移動終端。因此，基於圖 6，如圖 9 所示，在本發明提供的又一實施例中，本發明提供的基於移動終端卡模擬的信用支付方法，在步驟 S210 之前，還可以包括如下步驟：

在步驟 S207 中，接收移動終端發送的獲取預設安裝檔的請求。

其中，預設安裝檔包括：信用支付安裝檔。

在步驟 S208 中，根據獲取預設安裝檔的請求將預設安裝檔發送給移動終端，隨後執行步驟 S210。

下面首先對移動終端在支付交易時與交易終端之間的資料交互進行說明。

為了解決相關技術問題，本發明實施例提供了一種基於移動終端卡模擬的信用支付方法，應用於移動終端側，如圖 10 所示，該方法可以包括如下步驟：

在步驟 110 中，當檢測到交易終端時，向交易終端發送交易資訊。

為了便於說明，以交易終端為公交閘機為例進行說明。

在用戶手持移動終端貼近公交閘機進行支付交易時，由於公交閘機上能夠產生射頻場，當移動終端貼近公交閘機時，移動終端可以檢測到公交閘機產生的射頻場，進而可以檢測到公交閘機。在移動終端檢測到公交閘機時，移動終端向公交閘機發送交易資訊。

在步驟 120 中，接收交易終端發送的應用公鑰證書讀取指令。

在公交閘機接收到移動終端發送的交易資訊之後，公交閘機經過對該交易資訊的處理確認，會向移動終端發送應用公鑰證書讀取指令。移動終端在接收到公交閘機發送

的應用公鑰證書讀取指令之後，移動終端中的信用支付應用會讀取預先生成並存放在移動終端中的應用公鑰證書。

在步驟 130 中，根據應用公鑰證書讀取指令將應用公鑰證書發送給交易終端。

移動終端中的信用支付應用根據應用公鑰證書讀取指令將讀取到的應用公鑰證書發送給公交閘機。

在步驟 140 中，接收交易終端根據交易資訊發送的本次支付交易的扣款資訊。

公交閘機在接收到移動終端發送的應用公鑰證書之後，會對該應用公鑰證書驗簽，生成本次支付交易的扣款資訊，並將該扣款資訊發送給移動終端，移動終端接收公交閘機發送的扣款資訊。

在步驟 150 中，根據扣款資訊和交易資訊，利用移動終端中安裝的信用支付應用生成支付授權許可。

移動終端生成的支付授權許可包括：簽名資料和 TAC（Transaction Authentication Code，交易驗證碼）。

在步驟 160 中，將支付授權許可發送給交易終端，以使交易終端根據接收到的支付授權許可完成本次支付交易。

公交閘機在接收到移動終端發送的支付授權許可後，會對該支付許可進行驗證，如果驗證正確，將確定完成本次支付交易。

本發明實施例提供的基於移動終端卡模擬的信用支付方法，在用戶利用移動終端與交易終端進行支付交易時，

在移動終端依據交易終端發送的相關指令資訊依次將交易資訊、應用公鑰證書及生成的支付授權許可分別發送給交易終端，交易終端根據移動終端發送的資訊完成本次支付交易。與相關技術存在的問題相比，本發明實施例提供的基於移動終端卡模擬的信用支付方法，用戶在利用移動終端與交易終端交易時，可以使移動終端和交易終端分別處於離線模式，並且可以對移動終端的用戶帳戶採用信用記帳消費，在用戶利用移動終端消費之後才進行結算，可以避免用戶採用現金交易時產生的資金損失風險。

為了詳細說明本發明實施例移動終端是如何生成支付授權許可，以便交易終端根據移動終端發送的授權許可完成本次支付交易，作為圖 10 方法的細化，在本發明的另一實施例中，如圖 11 所示，步驟 150 還可以包括如下步驟：

在步驟 151 中，根據扣款資訊，利用移動終端中儲存的應用私鑰生成簽名資料。

應用私鑰是預先生成的，並且儲存在移動終端中，信用支付應用利用該應用私鑰對扣款資訊簽名，生成簽名資料。其中，扣款資訊包括：扣款金額、本次支付交易日期、本次支付交易時間、本次支付交易進出站標誌和本次支付交易的網站資訊。

在步驟 152 中，根據扣款資訊和交易資訊，利用移動終端中預先生成的交易驗證碼 TAC 子密鑰生成 TAC。

根據扣款資訊和交易資訊，移動終端中的信用支付應

用對扣款金額、本次支付交易日期、本次支付交易時間、支付卡號、可用額度和信用額度加密，生成 TAC。其中，信用額度是信用授權系統授權給用戶在離線狀態下的最大可用金額。

在步驟 153 中，將簽名資料和 TAC 均作為支付授權許可。

信用支付應用可以將簽名資料和 TAC 作為支付授權許可分別發送給公交閘機，也可以將簽名資料和 TAC 作為信用授權許可一起發送給公交閘機。

另外，上述交易資訊，包括：支付卡號、可用額度、進出站標誌和上筆交易資訊。其中，支付卡號是信用授權系統為每一個用戶的信用支付應用生成的唯一特徵碼。可用額度是用戶當前可以使用的金額。並且 TAC 子密鑰是信用授權系統服務端使用 TAC 母密鑰根據卡號散列得到的。

基於圖 10，該方法還可以包括如下步驟：

在步驟 11 中，根據本次支付交易扣款資訊中的扣款金額，將交易資訊中的可用額度減去扣款金額，得到當前可用額度。

在步驟 12 中，將當前可用額度作為移動終端中對應用戶的可用額度。隨後執行步驟 150

為了詳細說明移動終端與交易終端之間的交易支付過程，本發明實施例提供的一種基於移動終端卡模擬的信用支付方法，在交易終端側的執行流程，如圖 12 所示，該

方法可以包括如下步驟：

在步驟 410 中，在接收移動終端發送的交易資訊後，向移動終端發送應用公鑰證書讀取指令。

公交閘機接收移動終端發送的交易資訊，該交易資訊包括：支付卡號、可用額度、進出站標誌和上筆交易資訊。公交閘機會對該交易資訊中的內容進行檢查，例如：檢查移動終端對應帳戶的可用額度、進出站標誌位等資訊。當檢查合格後，公家閘機會向移動終端發送應用公鑰證書讀取指令。

在步驟 420 中，接收預設移動終端發送的應用公鑰證書。

當公交閘機將應用公鑰證書讀取指令發送給移動終端之後，移動終端會根據該指令向公交閘機發送應用公鑰證書，公交閘機將移動終端發送的應用公鑰證書接收。

在步驟 430 中，利用交易終端本地儲存的信用授權公鑰對應用公鑰證書驗簽。

為了識別接收到的應用公鑰證書是否正確，以及為了使用公鑰證書中的相關資訊，需要利用信用授權公鑰對應用公鑰證書驗簽。其中，信用授權公鑰可以是預先儲存在公交閘機中。

在步驟 440 中，當驗簽過程中從應用公鑰證書中恢復出應用公鑰時，生成本次支付交易的扣款資訊。

公交閘機對移動終端發送的應用公鑰證書驗簽，如果驗簽不通過，那麼結束本次支付交易。如果從應用公鑰證

書中恢復出應用公鑰，說明驗簽通過，生成本次支付交易的扣款資訊。需要說明的是，本次支付交易的扣款資訊還可以說是扣款指令，目的在於移動終端接收到公交閘機發送的扣款資訊（扣款指令）後，生成支付授權許可。

本次支付交易的扣款資訊包括：扣款金額、本次支付交易日期、本次支付交易時間、本次支付交易進出站標誌和本次支付交易的網站資訊。其中，扣款金額是指公交閘機根據本次支付交易的進出站標誌等資訊計算得到。

在步驟 450 中，將扣款資訊發送給移動終端。

公交閘機將生成的扣款資訊發送給移動終端，使得移動終端在接收到該扣款資訊後，根據扣款資訊和交易資訊，利用移動終端中安裝的信用支付應用生成支付授權許可。

在步驟 460 中，當接收到支付授權許可時，根據支付授權許可確定本次支付交易完成。

支付授權許可包括：簽名資料和 TAC。公交閘機會對支付授權許可中的簽名資料驗簽，如果驗簽未通過，那麼結束本次支付交易，如果驗簽通過記錄本次支付交易的交易日誌。

為了詳細說明本發明實施例交易終端如何根據移動終端發送的授權許可完成本次支付交易，作為圖 12 方法的細化，在本發明的另一實施例中，如圖 13 所示，步驟 460 還可以包括如下步驟：

在步驟 461 中，利用應用公鑰對簽名資料驗簽。

應用公鑰是公交閘機從移動終端發送的支付授權許可中恢復出而得到的，應用公鑰會檢查簽名資料中的相關資訊是否與應用公鑰中對應的資訊是否匹配，如果匹配，確定驗簽通過。

在步驟 462 中，當簽名資料驗簽成功時，生成交易日誌。

當公交閘機對簽名資料驗簽通過之後，生成本次支付的交易日誌。其中，交易日誌包括：扣款金額、交易日期、交易時刻、交易終端 ID、支付卡號、可用額度和 TAC。

在步驟 463 中，將交易日誌發送給預設伺服器，以使得預設伺服器根據交易日誌扣除移動終端對應的用戶帳戶中相應的金額。

如圖 14 所示，在本發明提供的又一實施例中，本發明實施例中提供的基於移動終端卡模擬的信用支付方法在交易終端側的執行流程還可以包括如下步驟：

在步驟 470 中，判斷交易資訊中的可用額度是否大於或者等於預設閾值。

如果可用額度大於或者等於預設閾值，執行步驟 480。

在步驟 470 中，檢查所述交易資訊中的進出站標誌是否為已出站狀態。

如果所述進出站標誌為已出站狀態，執行步驟 410。

該步驟 470 主要是為了公交閘機根據移動終端發送的

交易資訊，檢查移動終端對應的用戶帳戶的可用額度是否足以支付本次支付交易所用的金額，如果可用額度不足，那麼拒絕本次支付交易，如果可用額度足夠，那麼公交閘機會檢查交易資訊中的進出站標誌是否為 0，如果進出站標誌不為 0，那麼拒絕本次支付交易；如果進出站標誌為 0，那麼繼續本次支付交易。需要說明的是，進出站標誌中 1 表示用戶手持移動終端為已進站狀態，那麼拒絕本次支付交易；進出站標誌中 0 表示用戶手持移動終端為已出站狀態，那麼表示可以結帳，進行本次支付交易。

其中，交易資訊，包括：支付卡號、可用額度、進出站標誌和上筆交易資訊。

在本發明提供的又一實施例中，如圖 15 所示，本發明提供的基於移動終端卡模擬的信用支付方法，在實施例中，以手機代表移動終端，信用授權系統的服務端代表伺服器進行說明，在手機開通信用支付功能時，手機中的信用授權系統應用、信用支付應用及信用授權系統的服務端之間的流程包括：

步驟 1001、獲取手機的設備參數資訊；

步驟 1002、上傳設備參數資訊；

步驟 1003、判斷手機收是否滿足開通信用支付的硬體條件；

步驟 1004、返回判斷結果；

步驟 1005、判斷結果是：展示開通信用支付應用介面；

步驟 1006、上傳用戶身份資訊；

步驟 1007、判斷手機收是否滿足開通信用支付的安全認證條件；

步驟 1008、返回判斷結果；

步驟 1009、用戶選擇開通信用支付應用；

步驟 1010、啟動信用支付應用；

步驟 1011、返回啟動成功結果；

步驟 1012、請求應用私鑰、應用公鑰證書和信用支付資料；

步驟 1013、生成一對公私鑰對，使用信用授權私鑰生成應用公鑰證書；生成支付卡；號、散列生成應用 TAC 子密鑰、子密鑰和信用支付資料；

步驟 1014、返回應用私鑰、應用公鑰證書和信用支付資料；

步驟 1015、發送應用私鑰、應用公鑰證書和信用支付資料；

步驟 1016、保存應用私鑰、應用公鑰證書和信用支付資料；

步驟 1017、返回個人化結果；

步驟 1018、發送信用支付開通結果；

步驟 1019、記錄開通結果；

步驟 1020、返回處理完成通知；

步驟 1021、提示用戶信用支付應用開通成功。

在本發明提供的又一實施例中，如圖 16 所示，本發

明提供的基於移動終端卡模擬的信用支付方法，移動終端在支付交易的過程中，移動終端與公交閘機之間的資料交互流程如下：

步驟 2001、公交閘機選擇信用授權系統應用；

步驟 2002、信用授權系統應用讀取需要返回的資料；

步驟 2003、信用授權系統應用返回支付卡號、可用額度、進出站標誌、上次交易資訊；

步驟 2004、公交閘機檢查可用額度、進出站標誌；檢查不通過，提示拒絕資訊；

步驟 2005、公交閘機計算扣款金額；

步驟 2006、公交閘機根據扣款金額、交易時間、進出站標誌和交易資訊進行扣款；

步驟 2007、信用授權系統應用生成支付授權許可，包括：簽名資料和 TAC；

步驟 2008、信用授權系統應用返回簽名資料和 TAC；

步驟 2009、公交閘機使用應用公鑰對資料簽名驗簽；驗簽通過，記錄交易日誌；驗簽不通過，提示拒絕資訊。

另外，如圖 17 所示，公交閘機還需要定期上傳交易日誌信用授權系統，以及更新黑名單列表。本發明提供的基於移動終端卡模擬的信用支付方法，公交閘機（交易終端）與信用授權系統的服務端之間的資料交互流程如下：

步驟 3001、定期上傳交易日誌；

步驟 3002、結算，查詢系統中的黑名單是否有更新，若有更新，準備黑名單列表返回；

步驟 3003、返回交易日誌接收結果和黑名單列表；

步驟 3004、檢查是否存在黑名單列表；

步驟 3005、公交閘機更新黑名單列表；

步驟 3006、更新；

步驟 3007、返回更新完成結果。

透過以上的方法實施例的描述，所屬領域的技術人員可以清楚地瞭解到本發明可借助軟體加必需的通用硬體平臺的方式來實現，當然也可以透過硬體，但很多情況下前者是更佳的實施方式。基於這樣的理解，本發明的技術方案本質上或者說對現有技術做出貢獻的部分可以以軟體產品的形式體現出來，該電腦軟體產品儲存在一個儲存媒體中，包括若干指令用以使得一台電腦設備（可以是個人電腦，伺服器，或者網路設備等）執行本發明各個實施例所述方法的全部或部分步驟。而前述的儲存媒體包括：唯讀記憶體（ROM）、隨機存取記憶體（RAM）、磁碟或者光碟等各種可以儲存程式碼的媒體。

本發明實施例中，上述是以在公交支付過程中的應用為例進行說明，可以理解的是，根據需要，可以在其它支付場景下應用，例如地鐵支付，離線購物支付場景中等。具體應用場景不做特別限制。

另外，作為對上述各實施例的實現，本發明實施例還

提供了一種基於移動終端卡模擬的信用支付裝置，該裝置位於移動終端中，如圖 18 所示，該裝置包括：應用授權請求發送單元 10、密鑰接收單元 20、密鑰保存單元 30、信用支付資料獲取請求發送單元 40、信用支付資料接收單元 50 和信用支付完成單元 60，其中，

應用授權請求發送單元 10，用於利用所述移動終端中的信用授權系統應用向預設伺服器發送應用授權請求；

密鑰接收單元 20，用於發送的應用公鑰證書和應用私鑰；

密鑰保存單元 30，用於將所述應用公鑰證書和所述應用私鑰保存到所述移動終端的信用支付應用中；

信用支付資料獲取請求發送單元 40，用於向所述預設伺服器發送信用支付資料獲取請求；

信用支付資料接收單元 50，用於接收所述預設伺服器發送的信用支付資料；

信用支付完成單元 60，用於根據所述信用支付資料開通所述移動終端的信用支付功能。

在本發明又一實施例中，基於圖 18，如圖 19 所示，該裝置還包括：

設備參數資訊獲取單元 71，用於獲取所述移動終端的設備參數資訊；

設備參數資訊發送單元 72，用於將所述設備參數資訊發送給所述預設伺服器，以使所述預設伺服器根據接收到的所述設備參數資訊判斷所述移動終端是否滿足開通信

用支付的硬體條件；

第一檢測單元 73，用於檢測是否接收到所述預設伺服器發送的信用支付開通資訊；

硬體條件確定單元 74，用於在接收到所述預設伺服器發送的信用支付開通資訊時，確定所述移動終端滿足開通信用支付的硬體條件。

在本發明又一實施例中，基於圖 18，如圖 20 所示，該裝置還包括：

用戶身份資訊獲取單元 75，用於獲取用戶身份資訊；

用戶身份資訊發送單元 76，用於將所述用戶身份資訊發送給所述預設伺服器，以使所述預設終端根據接收到的所述用戶身份資訊判斷所述移動終端是否滿足開通信用支付的安全認證條件；

第二檢測單元 77，用於檢測是否接收到所述預設伺服器發送的安全認證通過資訊；

安全認證條件確定單元 78，用於在接收到所述預設伺服器發送的安全認證通過資訊時，確定所述移動終端滿足開通信用支付的安全認證條件。

在本發明又一實施例中，基於圖 18，如圖 21 所示，該裝置還包括：

獲取預設安裝檔請求發送單元 81，用於向所述預設伺服器發送獲取預設安裝檔的請求；所述預設安裝檔包括：信用支付安裝檔；

預設安裝檔獲取單元 82，用於獲取所述預設伺服器發送的所述預設安裝檔；

安裝單元 83，用於將所述預設安裝檔安裝在所述移動終端中。

本發明實施例還提供了一種基於移動終端卡模擬的信用支付裝置，該裝置位於交易終端中，如圖 22 所示，該裝置包括：應用授權請求接收單元 11、密鑰生成單元 12、應用公鑰證書生成單元 13、資料發送單元 14、信用支付資料獲取請求接收單元 15、信用支付資料生成單元 16 和信用支付資料發送單元 17，其中，

應用授權請求接收單元 11，用於接收移動終端發送的應用授權請求；

密鑰生成單元 12，用於根據所述應用授權請求分別生成應用公鑰和應用私鑰；

應用公鑰證書生成單元 13，用於利用所述預設伺服器中保存的信用授權私鑰對所述應用公鑰簽名，生成應用公鑰證書；

資料發送單元 14，用於將所述應用公鑰證書和所述應用私鑰發送給所述移動終端；

信用支付資料獲取請求接收單元 15，用於接收所述移動終端發送的信用支付資料獲取請求；

信用支付資料生成單元 16，用於根據所述信用支付資料獲取請求，生成與所述移動終端相對應信用支付資料；

信用支付資料發送單元 17，用於將所述信用支付資料發送給所述移動終端，以使所述移動終端根據接收到的信用支付資料開通所述移動終端的信用支付功能。

在本發明又一實施例中，基於圖 22，如圖 23 所示，該裝置還包括：

設備參數資訊接收單元 91，用於接收所述移動終端發送的設備參數資訊；

第一判斷單元 92，用於根據所述設備參數資訊判斷所述移動終端是否滿足開通信用支付的硬體條件；

信用支付開通資訊發送單元 93，用於在所述移動終端滿足開通信用支付的硬體條件時，向所述移動終端發送信用支付開通資訊。

在本發明又一實施例中，基於圖 22，如圖 24 所示，該裝置還包括：

用戶身份資訊接收單元 94，用於接收所述移動終端發送的用戶身份資訊；

第二判斷單元 95，用於根據所述用戶身份資訊判斷所述移動終端是否滿足開通信用支付的安全認證條件；

安全認證通過資訊發送單元 96，用於在所述身份資訊滿足開通信用支付的安全認證條件時，向所述移動終端發送安全認證通過資訊。

在本發明又一實施例中，基於圖 19，如圖 25 所示，該裝置還包括：

預設安裝檔請求接收單元 97，用於接收所述移動終

端發送的獲取預設安裝檔的請求，所述預設安裝檔包括：信用支付安裝檔；

預設安裝檔發送單元 98，用於根據所述獲取預設安裝檔的請求將所述預設安裝檔發送給所述移動終端。

關於上述實施例中的裝置，其中各個模組執行操作的具體方式已經在有關該方法的實施例中進行了詳細描述，此處將不做詳細闡述說明。

本發明提供的基於移動終端卡模擬的信用支付方法及裝置，可以應用在移動終端和交易終端中，當用戶開通支付應用之後，可以透過使用移動終端就可以完成對交易終端的離線信用支付，可以快速、安全的完成支付交易，並且無需線上支付，避免了相關技術中，例如用戶在乘坐公共交通工具時，還需要用戶使用現金或公交卡等方式才能實現支付交易功能。

可以理解的是，本發明可用於眾多通用或專用的計算系統環境或配置中。例如：個人電腦、伺服器電腦、手持設備或可攜式設備、平板型設備、多處理器系統、基於微處理器的系統、機頂盒、可程式設計的消費電子設備、網路 PC、小型電腦、大型電腦、包括以上任何系統或設備的分散式運算環境等等。

本發明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

發明，在這些分散式運算環境中，由透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儲存媒體中。

需要說明的是，在本文中，諸如“第一”和“第二”等之類的關係術語僅僅用來將一個實體或者操作與另一個實體或操作區分開來，而不一定要求或者暗示這些實體或操作之間存在任何這種實際的關係或者順序。而且，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、物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、物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、物品或者設備中還存在另外的相同要素。

本領域技術人員在考慮說明書及實踐這裡公開的發明後，將容易想到本發明的其它實施方案。本申請旨在涵蓋本發明的任何變型、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發明的一般性原理並包括本發明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，本發明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，本發明並不侷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。本發明的範圍僅由所附的申請專利範圍來限制。

【符號說明】

100：移動終端

200：交易終端

300：伺服器

10：應用授權請求發送單元

20：密鑰接收單元

30：密鑰保存單元

40：信用支付資料獲取請求發送單元

50：信用支付資料接收單元

60：信用支付完成單元

71：設備參數資訊獲取單元

72：設備參數資訊發送單元

73：第一檢測單元

74：硬體條件確定單元

75：用戶身份資訊獲取單元

76：用戶身份資訊發送單元

77：第二檢測單元

78：安全認證條件確定單元

81：獲取預設安裝檔請求發送單元

82：預設安裝檔獲取單元

83：安裝單元

11：應用授權請求接收單元

12：密鑰生成單元

13：應用公鑰證書生成單元

14：資料發送單元

15：信用支付資料獲取請求接收單元

16：信用支付資料生成單元

17：信用支付資料發送單元

91：設備參數資訊接收單元

92：第一判斷單元

93：信用支付開通資訊發送單元

94：用戶身份資訊接收單元

95：第二判斷單元

96：安全認證通過資訊發送單元

97：預設安裝檔請求接收單元

98：預設安裝檔發送單元

申請專利範圍

1. 一種基於移動終端卡模擬的信用支付方法，應用於移動終端，其特徵在於，該方法包括：

向預設伺服器發送應用授權請求；

接收該預設伺服器發送的應用公鑰證書和應用私鑰；

將該應用公鑰證書和該應用私鑰保存到該移動終端的信用支付應用中；

向該預設伺服器發送信用支付資料獲取請求；

接收該預設伺服器發送的信用支付資料，並根據該信用支付資料開通該移動終端的信用支付功能。

2. 根據申請專利範圍第 1 項所述的基於移動終端卡模擬的信用支付方法，其中，還包括：

獲取該移動終端的設備參數資訊；

將該設備參數資訊發送給該預設伺服器，以使該預設伺服器根據接收到的該設備參數資訊判斷該移動終端是否滿足開通信用支付的硬體條件；

檢測是否接收到該預設伺服器發送的信用支付開通資訊；

當接收到該預設伺服器發送的信用支付開通資訊時，確定該移動終端滿足開通信用支付的硬體條件，並執行所述向預設伺服器發送應用授權請求的步驟。

3. 根據申請專利範圍第 1 項所述的基於移動終端卡模擬的信用支付方法，其中，還包括：

獲取用戶身份資訊；

將該用戶身份資訊發送給該預設伺服器，以使該預設終端根據接收到的該用戶身份資訊判斷該移動終端是否滿足開通信用支付的安全認證條件；

檢測是否接收到該預設伺服器發送的安全認證通過資訊；

當接收到該預設伺服器發送的安全認證通過資訊時，確定該移動終端滿足開通信用支付的安全認證條件，並執行所述向預設伺服器發送應用授權請求的步驟。

4. 根據申請專利範圍第 1 項所述的基於移動終端卡模擬的信用支付方法，其中，還包括：

向該預設伺服器發送獲取預設安裝檔的請求；該預設安裝檔包括：信用支付安裝檔；

獲取該預設伺服器發送的該預設安裝檔；

將該預設安裝檔安裝在該移動終端中，執行所述向預設伺服器發送應用授權請求的步驟。

5. 根據申請專利範圍第 1 項所述的基於移動終端卡模擬的信用支付方法，其中，該信用支付資料，包括：支付卡號、信用額度、可用額度和交易驗證碼 TAC 子密鑰。

6. 一種基於移動終端卡模擬的信用支付方法，應用於伺服器，其特徵在於，該方法包括：

接收移動終端發送的應用授權請求；

根據該應用授權請求分別生成應用公鑰和應用私鑰；

利用該預設伺服器中保存的信用授權私鑰對該應用公

鑰簽名，生成應用公鑰證書；

將該應用公鑰證書和該應用私鑰發送給該移動終端；

接收該移動終端發送的信用支付資料獲取請求；

根據該信用支付資料獲取請求，生成與該移動終端相對應信用支付資料，並將該信用支付資料發送給該移動終端，以使該移動終端根據接收到的該信用支付資料開通該移動終端的信用支付功能。

7. 根據申請專利範圍第 6 項所述的基於移動終端卡模擬的信用支付方法，其中，還包括：

接收該移動終端發送的設備參數資訊；

根據該設備參數資訊判斷該移動終端是否滿足開通信用支付的硬體條件；

當該移動終端滿足開通信用支付的硬體條件時，向該移動終端發送信用支付開通資訊，並執行所述接收移動終端發送的應用授權請求的步驟。

8. 根據申請專利範圍第 6 項所述的基於移動終端卡模擬的信用支付方法，其中，還包括：

接收該移動終端發送的用戶身份資訊；

根據該用戶身份資訊判斷該移動終端是否滿足開通信用支付的安全認證條件；

當該身份資訊滿足開通信用支付的安全認證條件時，向該移動終端發送安全認證通過資訊，並執行所述接收移動終端發送的應用授權請求的步驟。

9. 根據申請專利範圍第 6 項所述的基於移動終端卡

模擬的信用支付方法，其中，還包括：

接收該移動終端發送的獲取預設安裝檔的請求，該預設安裝檔包括：信用支付安裝檔；

根據該獲取預設安裝檔的請求將該預設安裝檔發送給該移動終端，並執行所述接收移動終端發送的應用授權請求的步驟。

10. 一種基於移動終端卡模擬的信用支付裝置，應用於移動終端，其特徵在於，該裝置包括：

應用授權請求發送單元，用於向預設伺服器發送應用授權請求；

密鑰接收單元，用於接收該預設伺服器發送的應用公鑰證書和應用私鑰；

密鑰保存單元，用於將該應用公鑰證書和該應用私鑰保存到該移動終端的信用支付應用中；

信用支付資料獲取請求發送單元，用於向該預設伺服器發送信用支付資料獲取請求；

信用支付資料接收單元，用於接收該預設伺服器發送的信用支付資料；

信用支付完成單元，用於根據該信用支付資料開通所述移動終端的信用支付功能。

11. 根據申請專利範圍第 10 項所述的基於移動終端卡模擬的信用支付裝置，其中，還包括：

設備參數資訊獲取單元，用於獲取該移動終端的設備參數資訊；

設備參數資訊發送單元，用於將該設備參數資訊發送給該預設伺服器，以使該預設伺服器根據接收到的該設備參數資訊判斷該移動終端是否滿足開通信用支付的硬體條件；

第一檢測單元，用於檢測是否接收到該預設伺服器發送的信用支付開通資訊；

硬體條件確定單元，用於在接收到該預設伺服器發送的信用支付開通資訊時，確定該移動終端滿足開通信用支付的硬體條件。

12. 根據申請專利範圍第 10 項所述的基於移動終端卡模擬的信用支付裝置，其中，還包括：

用戶身份資訊獲取單元，用於獲取用戶身份資訊；

用戶身份資訊發送單元，用於將該用戶身份資訊發送給該預設伺服器，以使該預設終端根據接收到的該用戶身份資訊判斷該移動終端是否滿足開通信用支付的安全認證條件；

第二檢測單元，用於檢測是否接收到該預設伺服器發送的安全認證通過資訊；

安全認證條件確定單元，用於在接收到該預設伺服器發送的安全認證通過資訊時，確定該移動終端滿足開通信用支付的安全認證條件。

13. 根據申請專利範圍第 10 項所述的基於移動終端卡模擬的信用支付裝置，其中，還包括：

獲取預設安裝檔請求發送單元，用於向該預設伺服器

發送獲取預設安裝檔的請求；該預設安裝檔包括：信用支付安裝檔；

預設安裝檔獲取單元，用於獲取該預設伺服器發送的該預設安裝檔；

安裝單元，用於將該預設安裝檔安裝在該移動終端中。

14. 根據申請專利範圍第 10 項所述的基於移動終端卡模擬的信用支付裝置，其中，該信用支付資料，包括：支付卡號、信用額度、可用額度和交易驗證碼 TAC 子密鑰。

15. 一種基於移動終端卡模擬的信用支付裝置，應用於伺服器，其特徵在於，該裝置包括：

應用授權請求接收單元，用於接收移動終端發送的應用授權請求；

密鑰生成單元，用於根據該應用授權請求分別生成應用公鑰和應用私鑰；

應用公鑰證書生成單元，用於利用該預設伺服器中保存的信用授權私鑰對該應用公鑰簽名，生成應用公鑰證書；

資料發送單元，用於將該應用公鑰證書和該應用私鑰發送給該移動終端；

信用支付資料獲取請求接收單元，用於接收該移動終端發送的信用支付資料獲取請求；

信用支付資料生成單元，用於根據該信用支付資料獲

取請求，生成與該移動終端相對應信用支付資料；

信用支付資料發送單元，用於將該信用支付資料發送給該移動終端，以使該移動終端根據接收到的該信用支付資料開通該移動終端的信用支付功能。

16. 根據申請專利範圍第 15 項所述的基於移動終端卡模擬的信用支付裝置，其中，還包括：

設備參數資訊接收單元，用於接收該移動終端發送的設備參數資訊；

第一判斷單元，用於根據該設備參數資訊判斷該移動終端是否滿足開通信用支付的硬體條件；

信用支付開通資訊發送單元，用於在該移動終端滿足開通信用支付的硬體條件時，向該移動終端發送信用支付開通資訊。

17. 根據申請專利範圍第 15 項所述的基於移動終端卡模擬的信用支付裝置，其中，還包括：

用戶身份資訊接收單元，用於接收該移動終端發送的用戶身份資訊；

第二判斷單元，用於根據該用戶身份資訊判斷該移動終端是否滿足開通信用支付的安全認證條件；

安全認證通過資訊發送單元，用於在該身份資訊滿足開通信用支付的安全認證條件時，向該移動終端發送安全認證通過資訊。

18. 根據申請專利範圍第 15 項所述的基於移動終端卡模擬的信用支付裝置，其中，還包括：

預設安裝檔請求接收單元，用於接收該移動終端發送的獲取預設安裝檔的請求，該預設安裝檔包括：信用支付安裝檔；

預設安裝檔發送單元，用於根據該獲取預設安裝檔的請求將該預設安裝檔發送給該移動終端。

圖　式

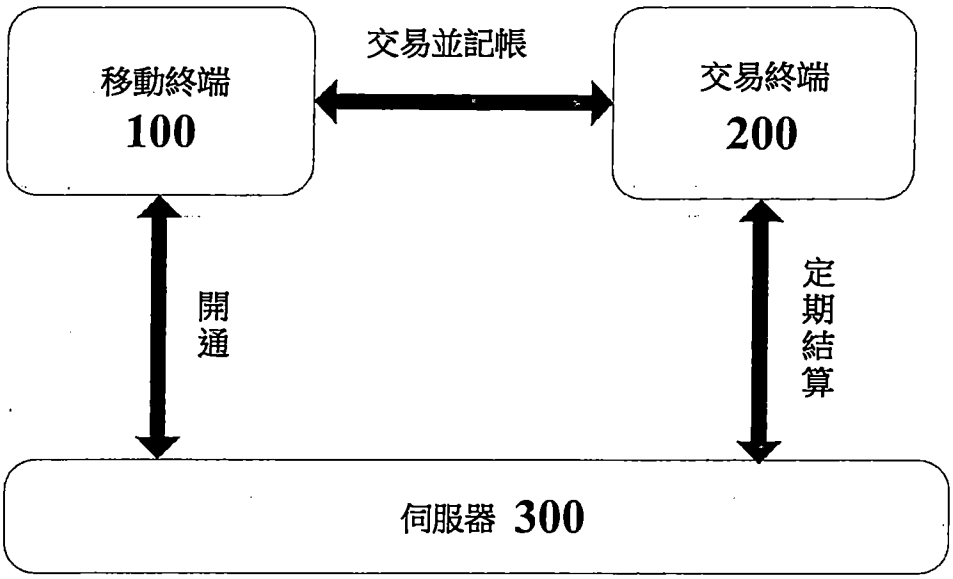
移動終端
100
交易並記帳
交易終端
200
開通
定期結算
伺服器 300

圖 1

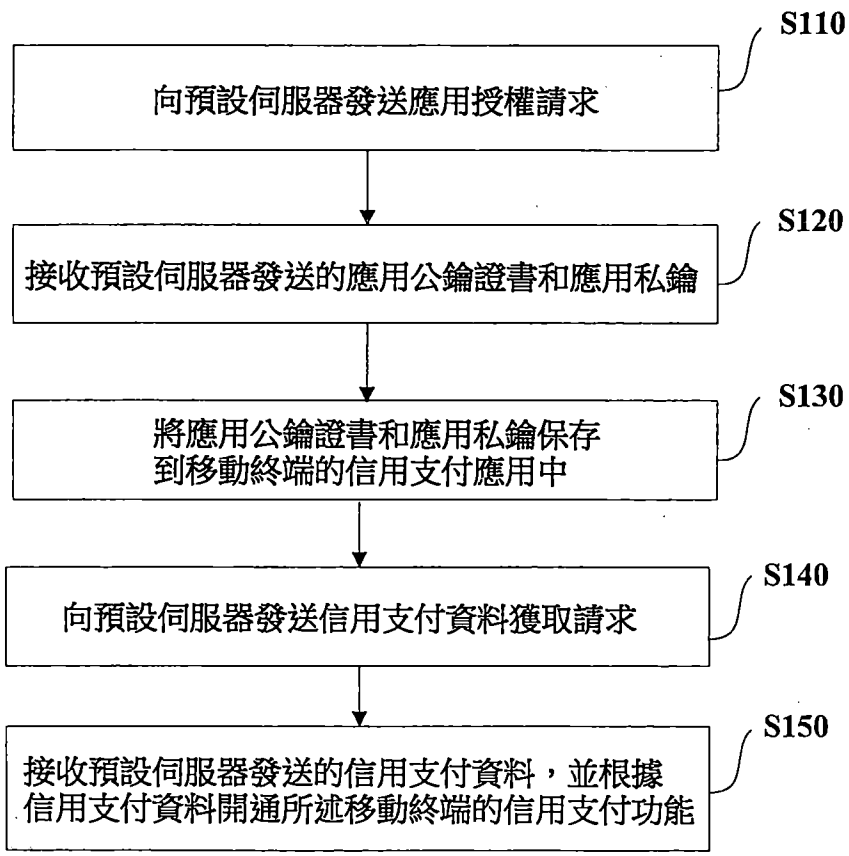
S110
向預設伺服器發送應用授權請求
S120
接收預設伺服器發送的應用公鑰證書和應用私鑰
S130
將應用公鑰證書和應用私鑰保存到移動終端的信用支付應用中
S140
向預設伺服器發送信用支付資料獲取請求
S150
接收預設伺服器發送的信用支付資料，並根據信用支付資料開通所述移動終端的信用支付功能

圖 2

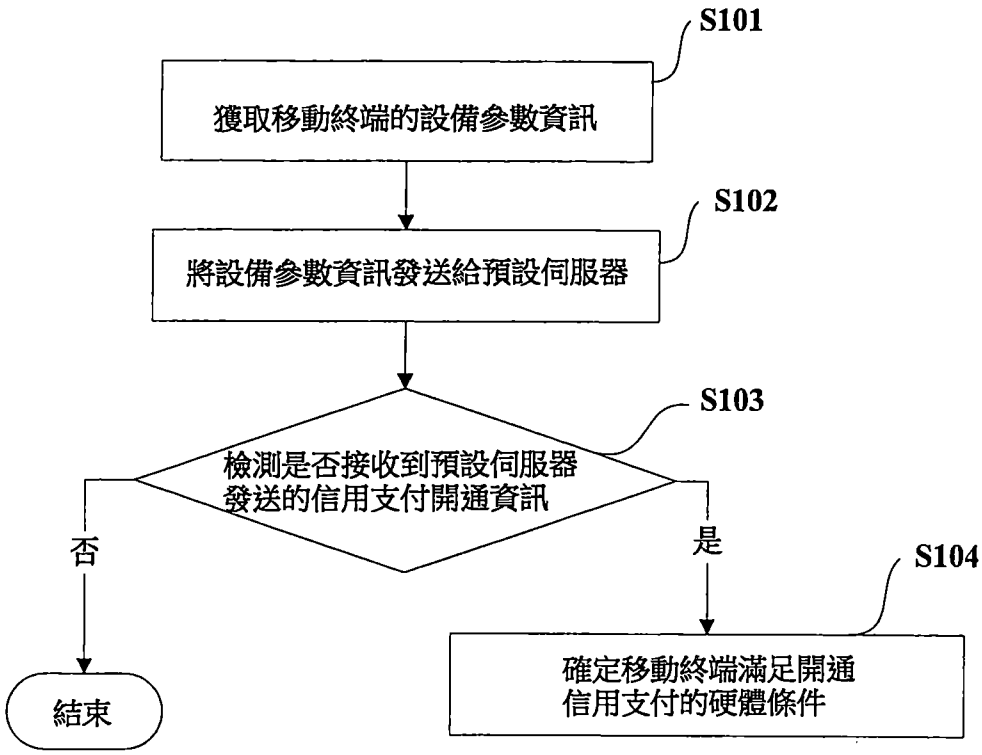
S101
獲取移動終端的設備參數資訊
S102
將設備參數資訊發送給預設伺服器
S103
檢測是否接收到預設伺服器
發送的信用支付開通資訊
否
是
S104
結束
確定移動終端滿足開通
信用支付的硬體條件

圖 3

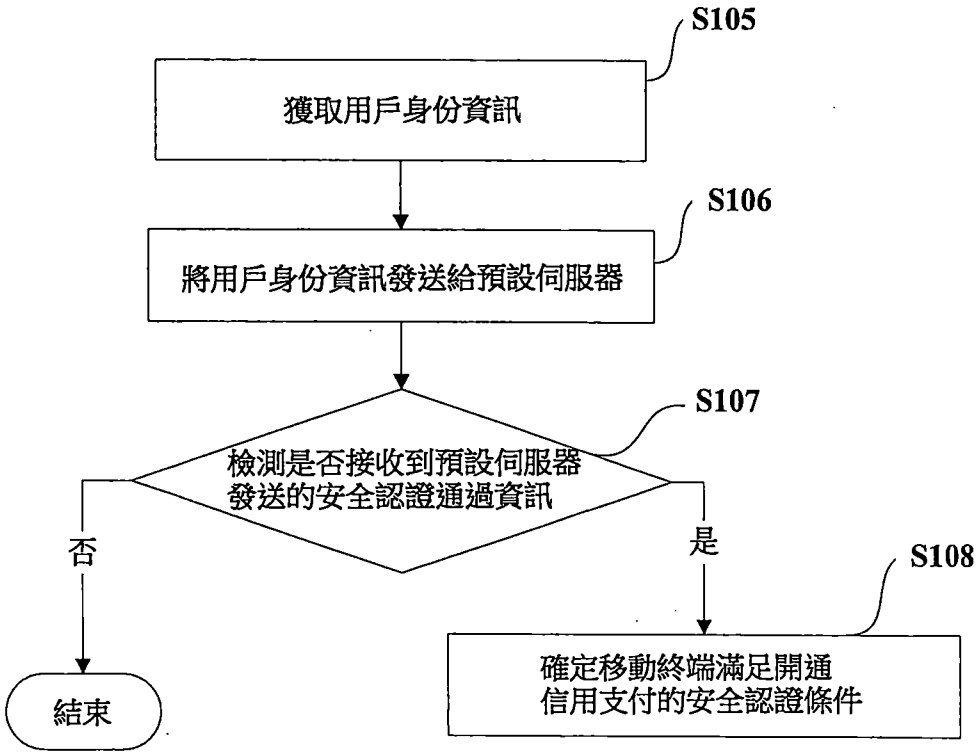
S105
獲取用戶身份資訊
S106
將用戶身份資訊發送給預設伺服器
S107
檢測是否接收到預設伺服器
發送的安全認證通過資訊
否
是
S108
結束
確定移動終端滿足開通
信用支付的安全認證條件

圖 4

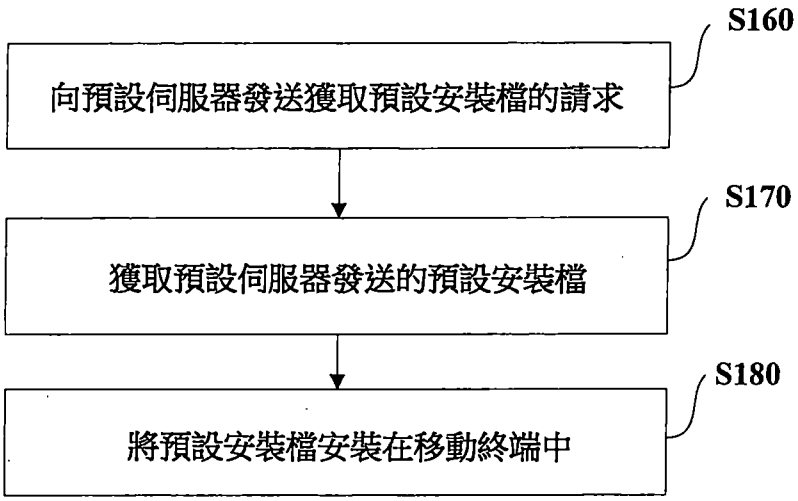
S160
向預設伺服器發送獲取預設安裝檔的請求
S170
獲取預設伺服器發送的預設安裝檔
S180
將預設安裝檔安裝在移動終端中

圖 5

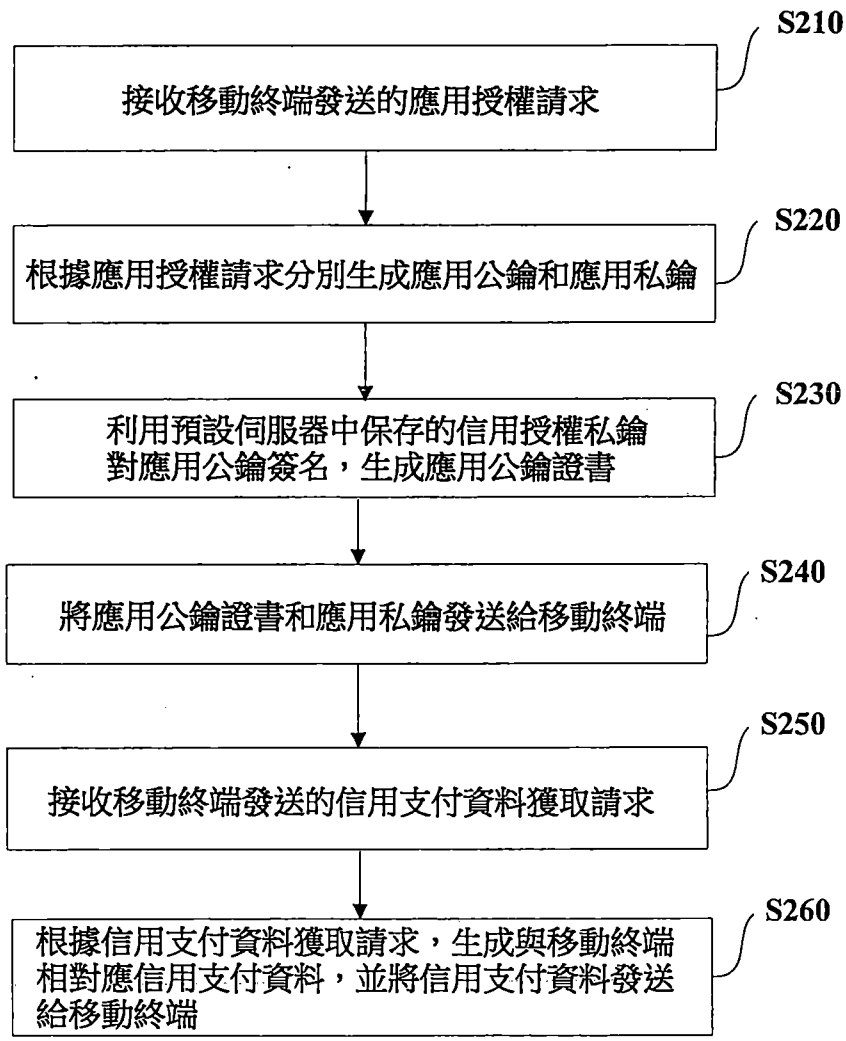
S210
接收移動終端發送的應用授權請求
S220
根據應用授權請求分別生成應用公鑰和應用私鑰
S230
利用預設伺服器中保存的信用授權私鑰
對應用公鑰簽名，生成應用公鑰證書
S240
將應用公鑰證書和應用私鑰發送給移動終端
S250
接收移動終端發送的信用支付資料獲取請求
S260
根據信用支付資料獲取請求，生成與移動終端
相對應信用支付資料，並將信用支付資料發送
給移動終端

圖 6

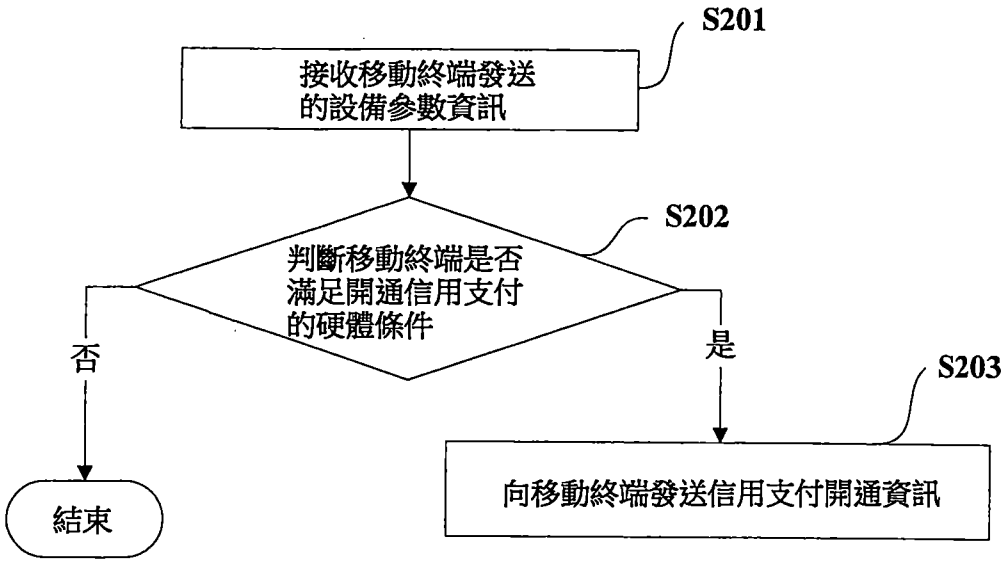
S201
接收移動終端發送
的設備參數資訊
S202
判斷移動終端是否
滿足開通信用支付
的硬體條件
否
是
S203
結束
向移動終端發送信用支付開通資訊

圖 7

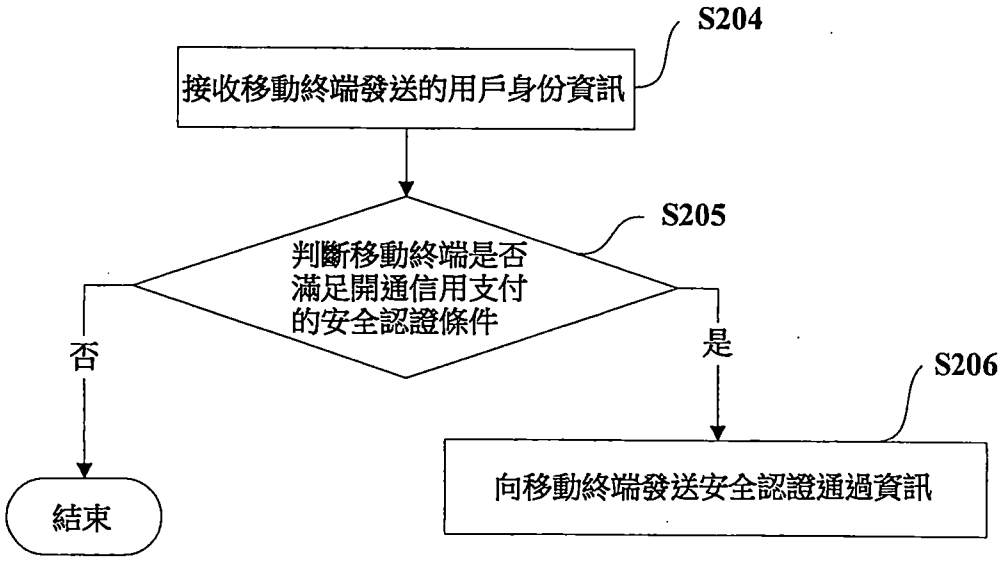
S204
接收移動終端發送的用戶身份資訊
S205
判斷移動終端是否
滿足開通信用支付
的安全認證條件
否
是
S206
結束
向移動終端發送安全認證通過資訊

圖 8

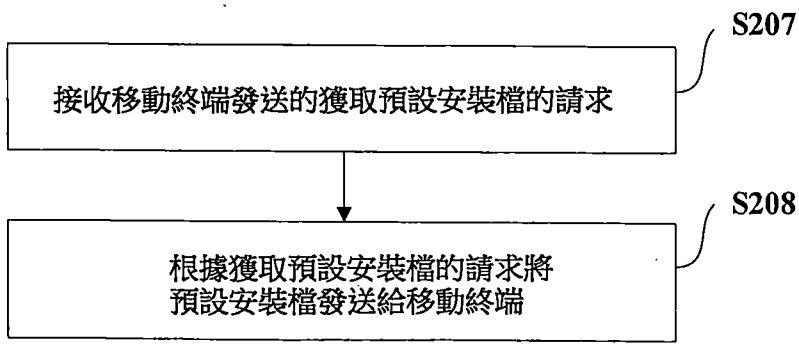
S207
接收移動終端發送的獲取預設安裝檔的請求
S208
根據獲取預設安裝檔的請求將
預設安裝檔發送給移動終端

圖 9

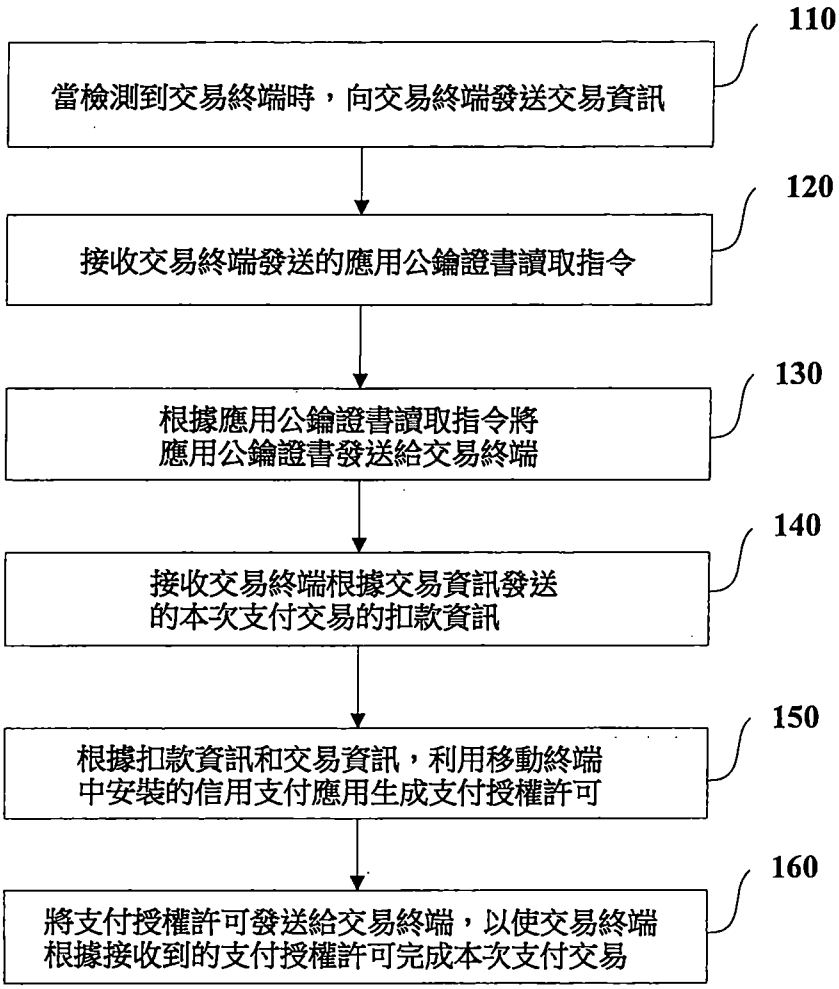
110
當檢測到交易終端時，向交易終端發送交易資訊
120
接收交易終端發送的應用公鑰證書讀取指令
130
根據應用公鑰證書讀取指令將
應用公鑰證書發送給交易終端
140
接收交易終端根據交易資訊發送
的本次支付交易的扣款資訊
150
根據扣款資訊和交易資訊，利用移動終端
中安裝的信用支付應用生成支付授權許可
160
將支付授權許可發送給交易終端，以使交易終端
根據接收到的支付授權許可完成本次支付交易

圖 10

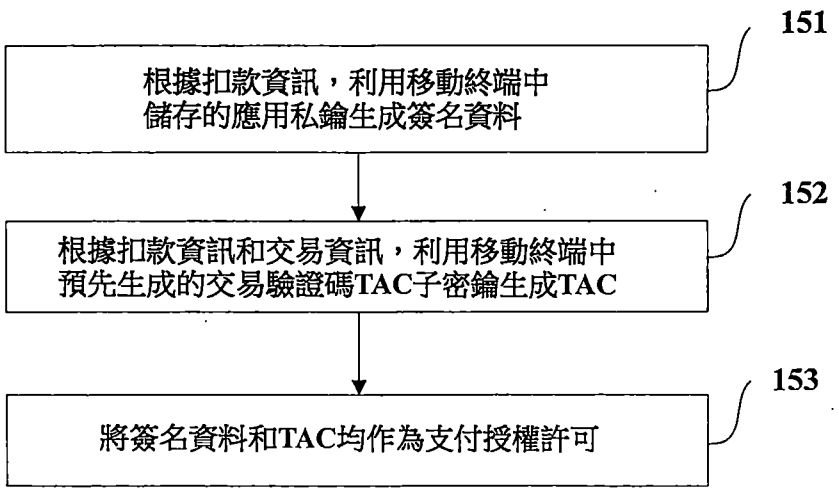
151
根據扣款資訊，利用移動終端中
儲存的應用私鑰生成簽名資料
152
根據扣款資訊和交易資訊，利用移動終端中
預先生成的交易驗證碼TAC子密鑰生成TAC
153
將簽名資料和TAC均作為支付授權許可

圖 11

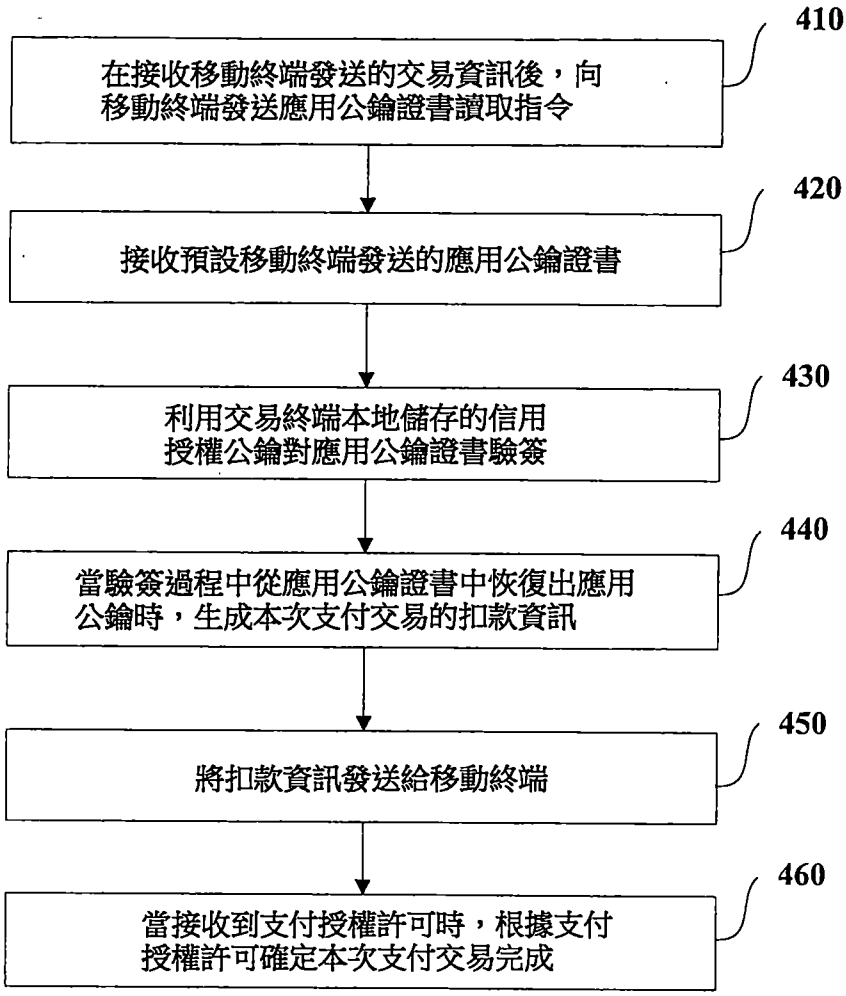
410
在接收移動終端發送的交易資訊後，向移動終端發送應用公鑰證書讀取指令
420
接收預設移動終端發送的應用公鑰證書
430
利用交易終端本地儲存的信用授權公鑰對應用公鑰證書驗簽
440
當驗簽過程中從應用公鑰證書中恢復出應用公鑰時，生成本次支付交易的扣款資訊
450
將扣款資訊發送給移動終端
460
當接收到支付授權許可時，根據支付授權許可確定本次支付交易完成

圖 12

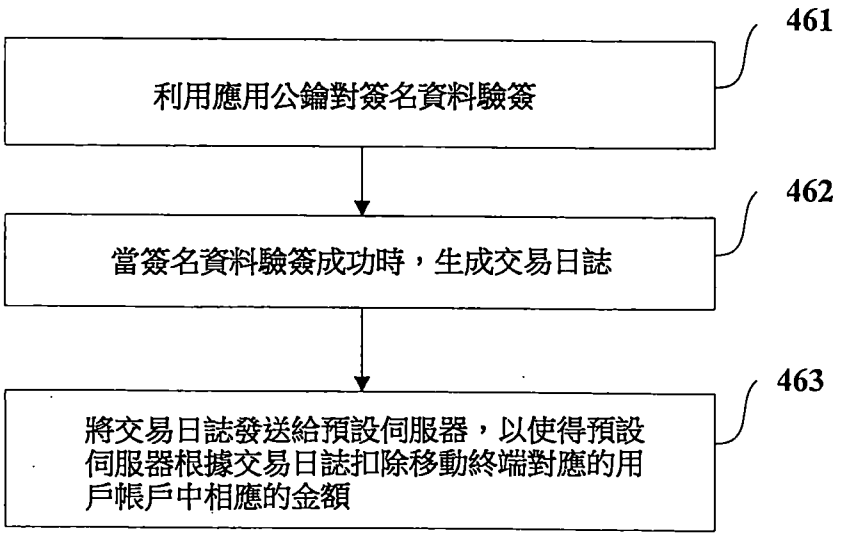
461
利用應用公鑰對簽名資料驗簽
462
當簽名資料驗簽成功時，生成交易日誌
463
將交易日誌發送給預設伺服器，以使得預設伺服器根據交易日誌扣除移動終端對應的用戶帳戶中相應的金額

圖 13

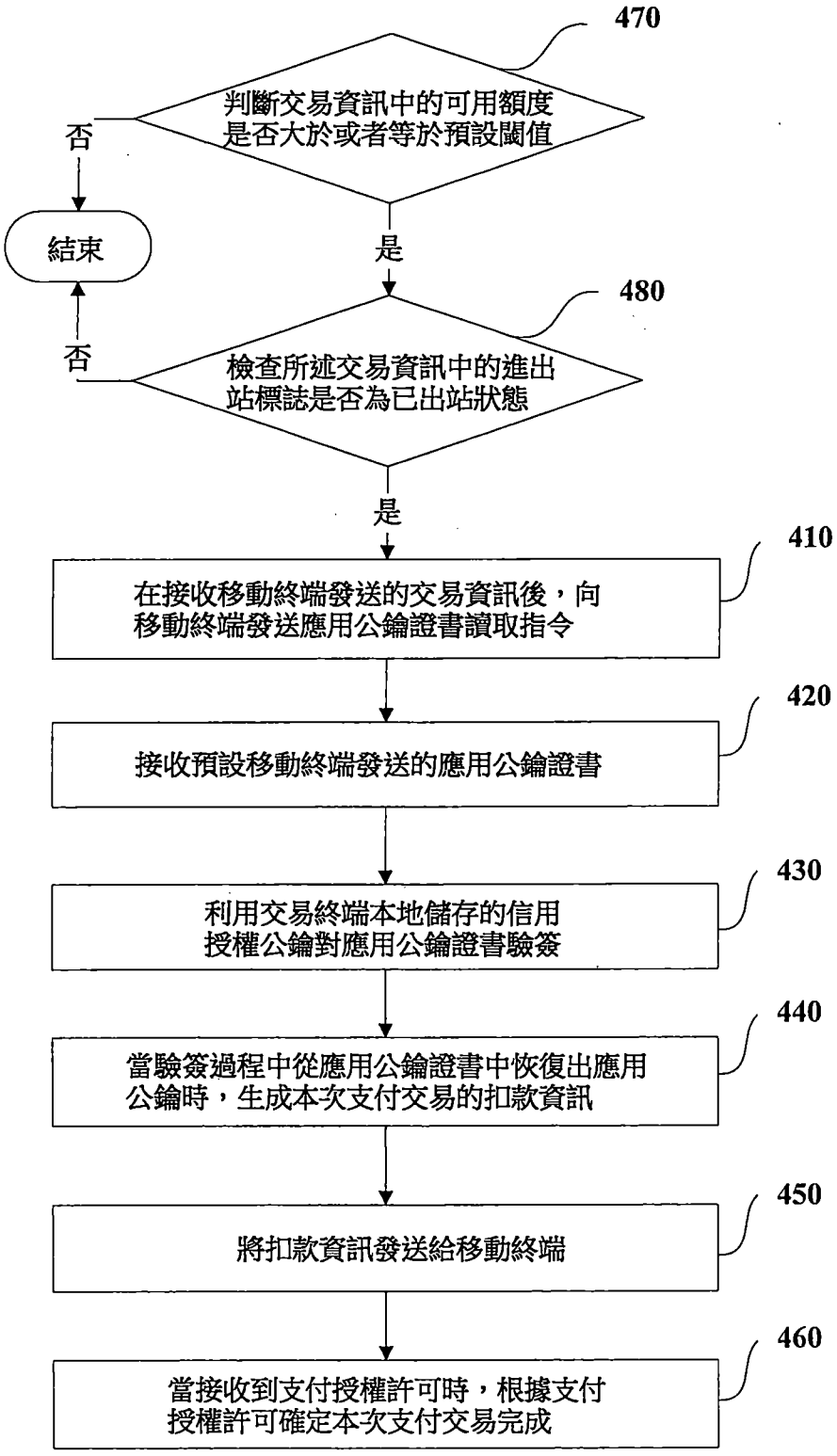
470
判斷交易資訊中的可用額度
是否大於或者等於預設閾值
否
結束
是
480
檢查所述交易資訊中的進出
站標誌是否為已出站狀態
否
是
410
在接收移動終端發送的交易資訊後，向
移動終端發送應用公鑰證書讀取指令
420
接收預設移動終端發送的應用公鑰證書
430
利用交易終端本地儲存的信用
授權公鑰對應用公鑰證書驗簽
440
當驗簽過程中從應用公鑰證書中恢復出應用
公鑰時，生成本次支付交易的扣款資訊
450
將扣款資訊發送給移動終端
460
當接收到支付授權許可時，根據支付
授權許可確定本次支付交易完成

圖 14

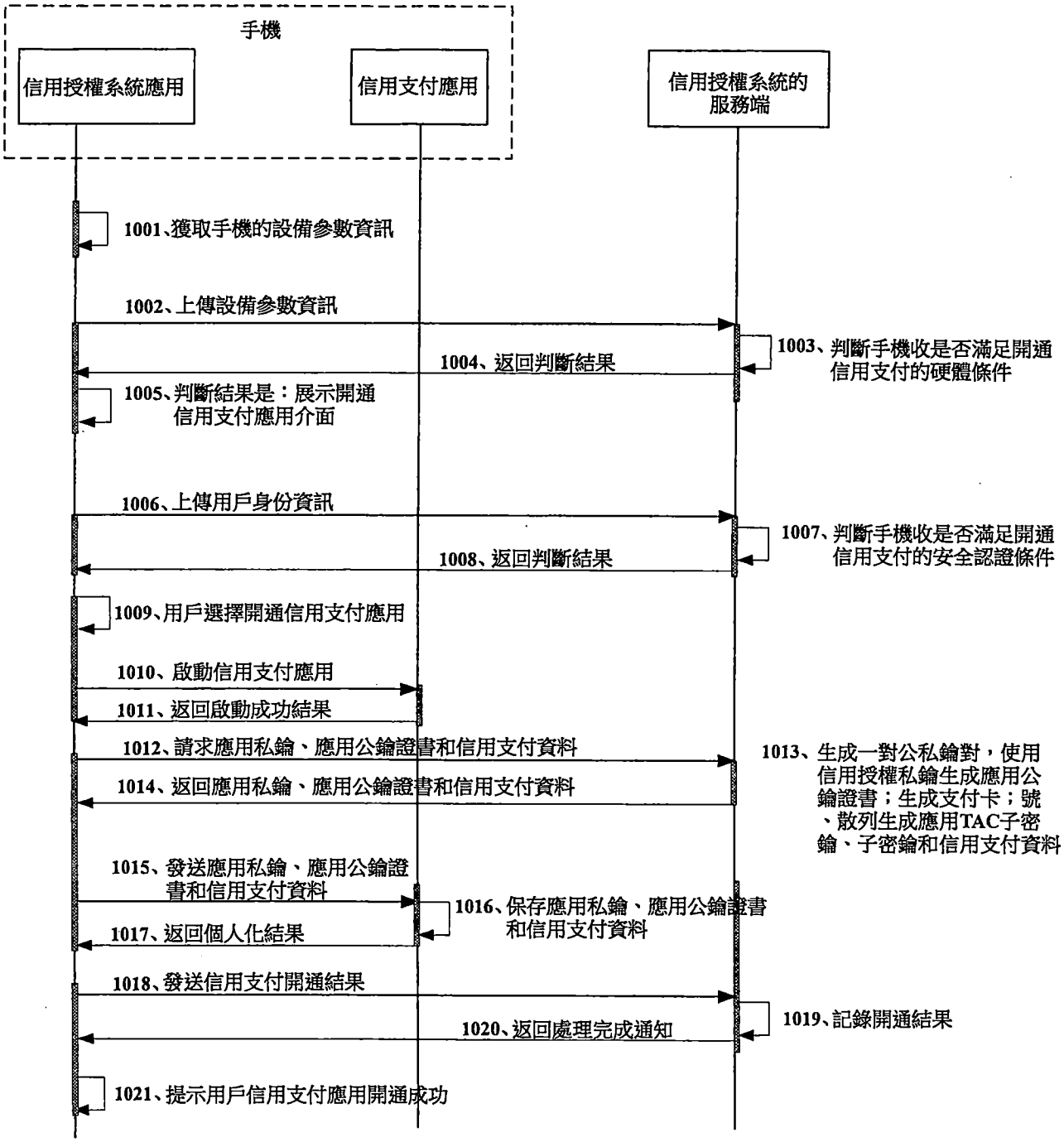
手機
信用授權系統應用
信用支付應用
信用授權系統的服務端
1001、獲取手機的設備參數資訊
1002、上傳設備參數資訊
1003、判斷手機收是否滿足開通信用支付的硬體條件
1004、返回判斷結果
1005、判斷結果是：展示開通信用支付應用介面
1006、上傳用戶身份資訊
1007、判斷手機收是否滿足開通信用支付的安全認證條件
1008、返回判斷結果
1009、用戶選擇開通信用支付應用
1010、啟動信用支付應用
1011、返回啟動成功結果
1012、請求應用私鑰、應用公鑰證書和信用支付資料
1013、生成一對公私鑰對，使用信用授權私鑰生成應用公鑰證書；生成支付卡；號、散列生成應用TAC子密鑰、子密鑰和信用支付資料
1014、返回應用私鑰、應用公鑰證書和信用支付資料
1015、發送應用私鑰、應用公鑰證書和信用支付資料
1016、保存應用私鑰、應用公鑰證書和信用支付資料
1017、返回個人化結果
1018、發送信用支付開通結果
1019、記錄開通結果
1020、返回處理完成通知
1021、提示用戶信用支付應用開通成功

圖 15

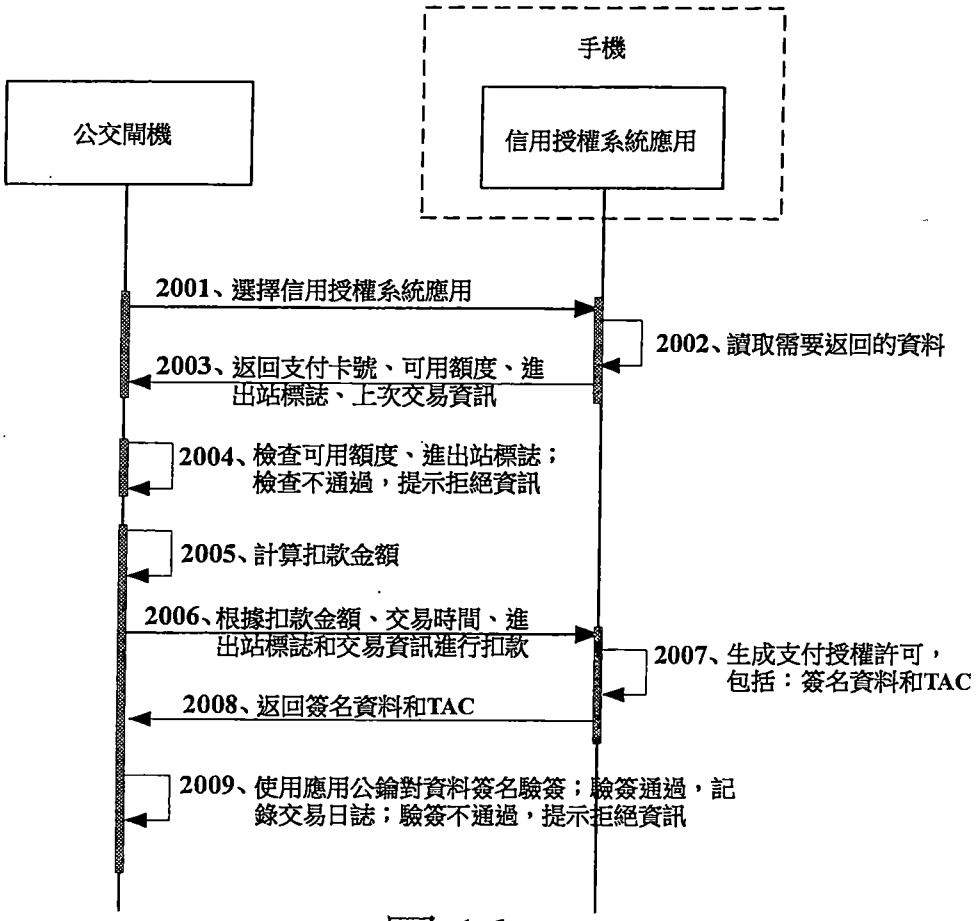
手機
公交閘機
信用授權系統應用
2001、選擇信用授權系統應用
2002、讀取需要返回的資料
2003、返回支付卡號、可用額度、進出站標誌、上次交易資訊
2004、檢查可用額度、進出站標誌；檢查不通過，提示拒絕資訊
2005、計算扣款金額
2006、根據扣款金額、交易時間、進出站標誌和交易資訊進行扣款
2007、生成支付授權許可，包括：簽名資料和TAC
2008、返回簽名資料和TAC
2009、使用應用公鑰對資料簽名驗簽；驗簽通過，記錄交易日誌；驗簽不通過，提示拒絕資訊

圖 16

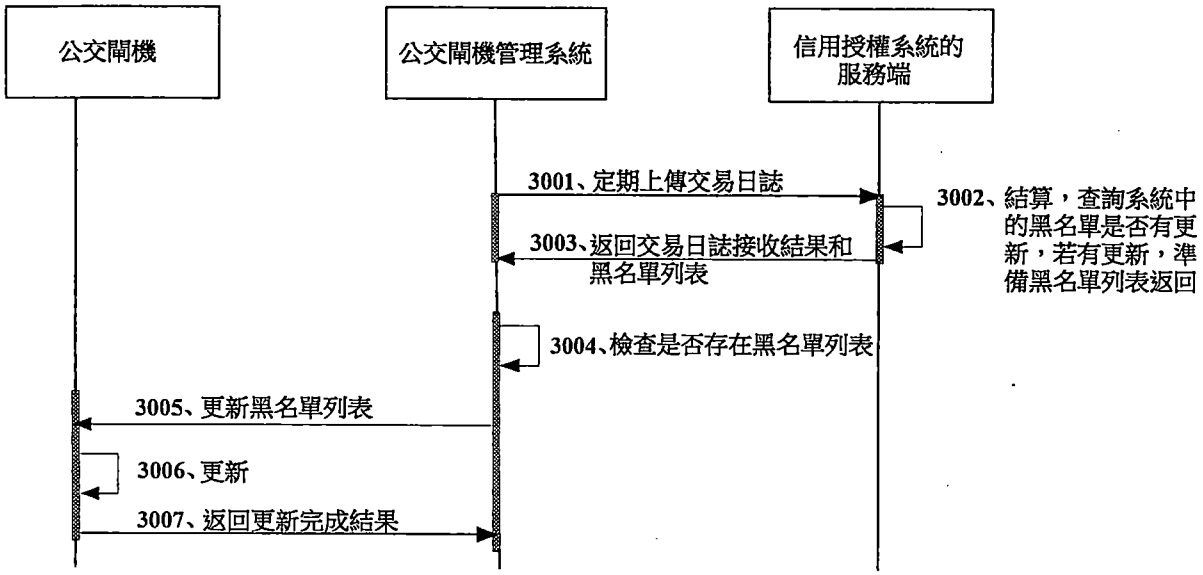
公交閘機
公交閘機管理系統
信用授權系統的服務端
3001、定期上傳交易日誌
3002、結算，查詢系統中的黑名單是否有更新，若有更新，準備黑名單列表返回
3003、返回交易日誌接收結果和黑名單列表
3004、檢查是否存在黑名單列表
3005、更新黑名單列表
3006、更新
3007、返回更新完成結果

圖 17

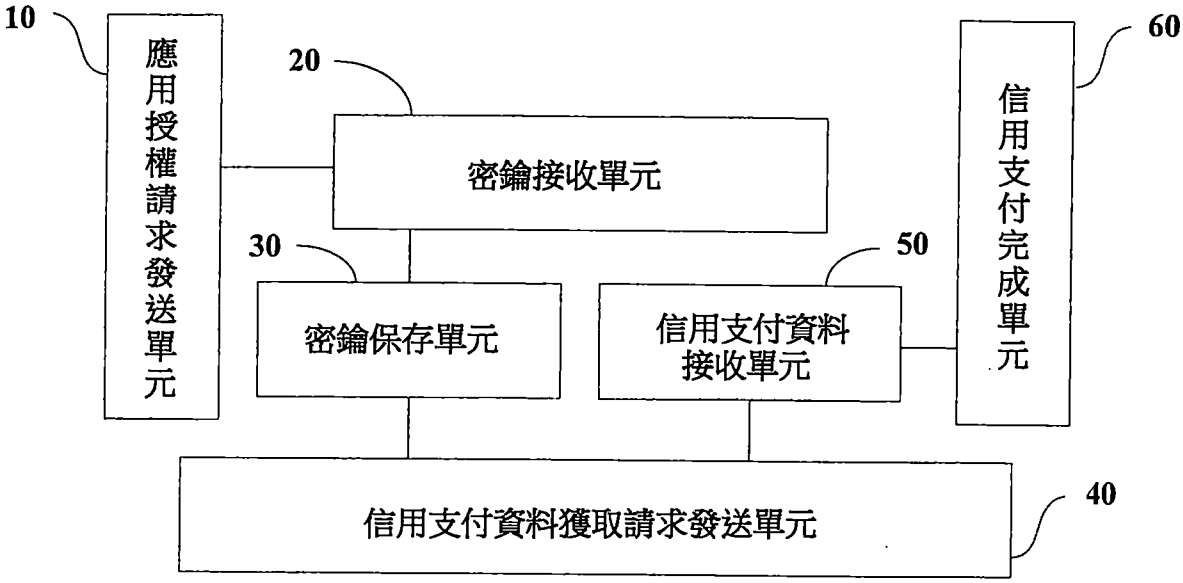
10
應用授權請求發送單元
20
密鑰接收單元
30
密鑰保存單元
50
信用支付資料接收單元
60
信用支付完成單元
信用支付資料獲取請求發送單元
40

圖 18

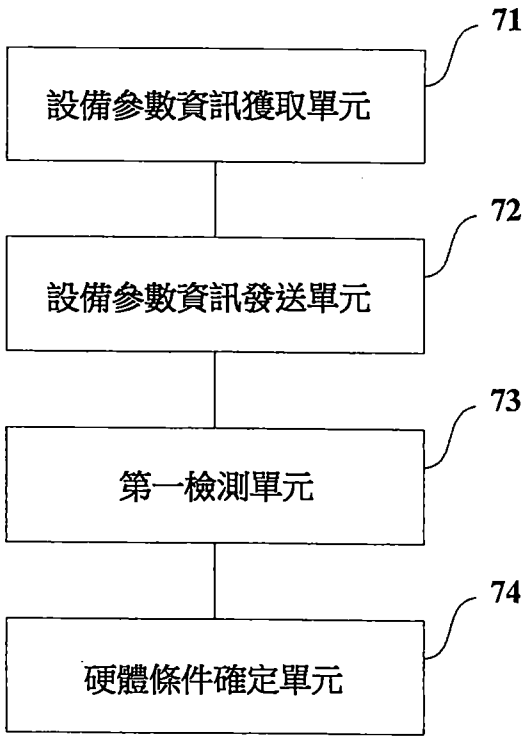
71
設備參數資訊獲取單元
72
設備參數資訊發送單元
73
第一檢測單元
74
硬體條件確定單元

圖 19

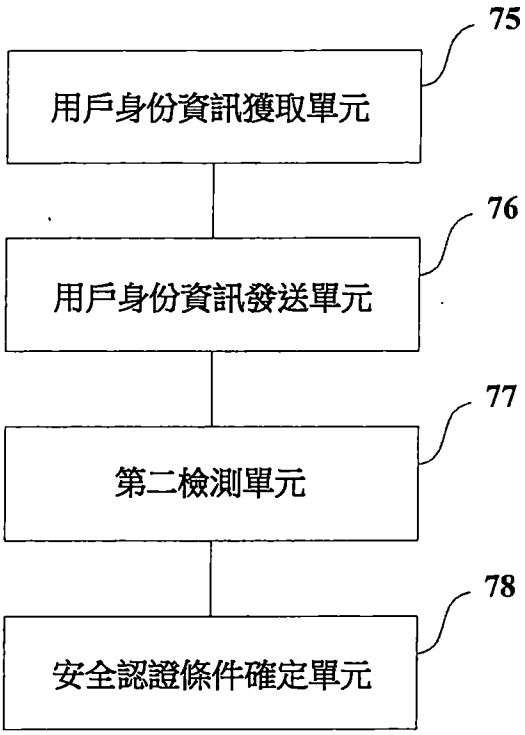
75
用戶身份資訊獲取單元
76
用戶身份資訊發送單元
77
第二檢測單元
78
安全認證條件確定單元

圖 20

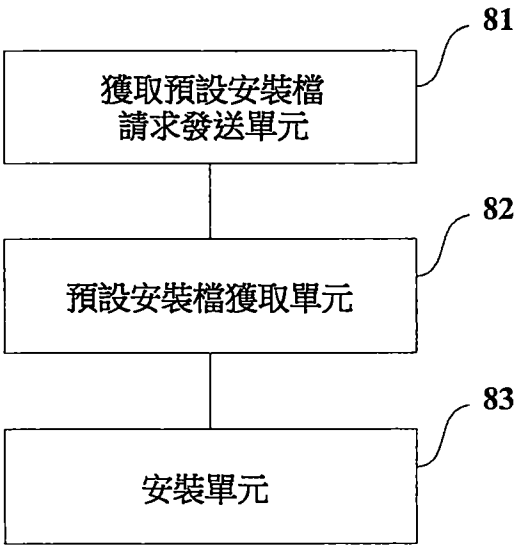
81
獲取預設安裝檔
請求發送單元
82
預設安裝檔獲取單元
83
安裝單元

圖 21

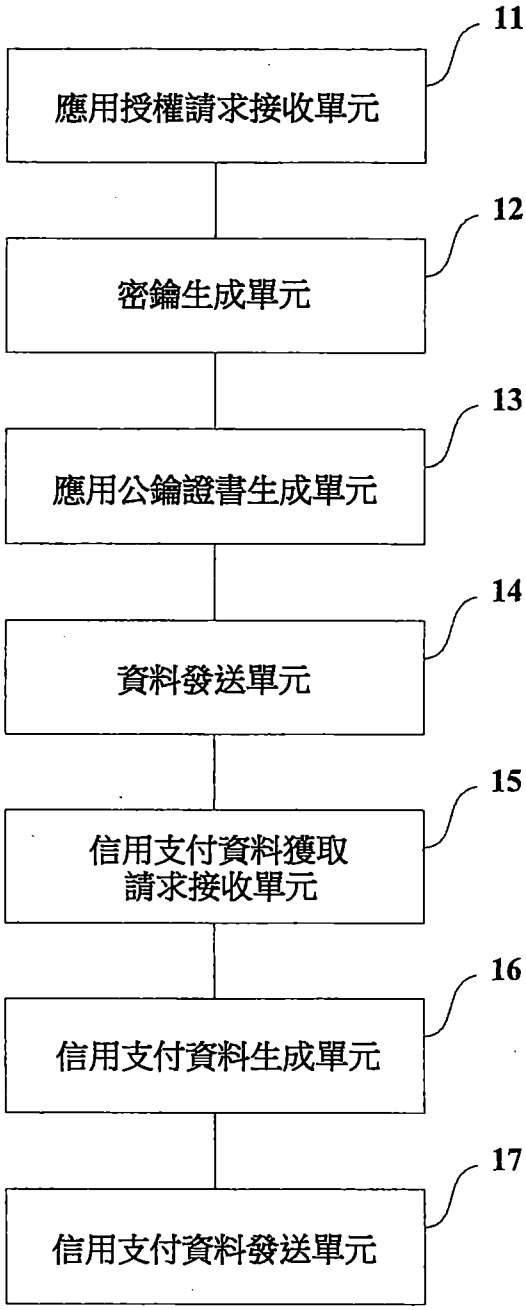
11
應用授權請求接收單元
12
密鑰生成單元
13
應用公鑰證書生成單元
14
資料發送單元
15
信用支付資料獲取
請求接收單元
16
信用支付資料生成單元
17
信用支付資料發送單元

圖 22

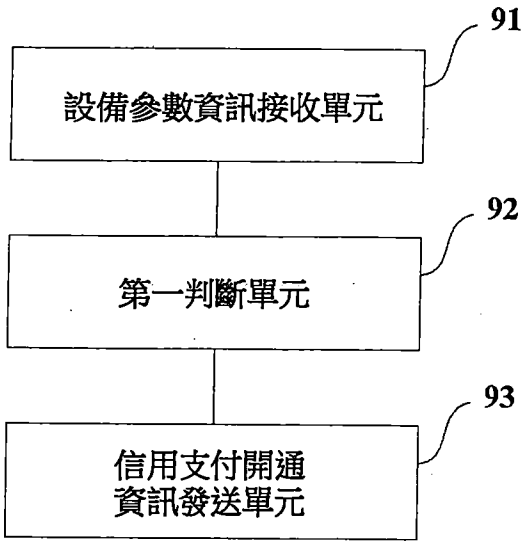
91
設備參數資訊接收單元
92
第一判斷單元
93
信用支付開通
資訊發送單元

圖 23

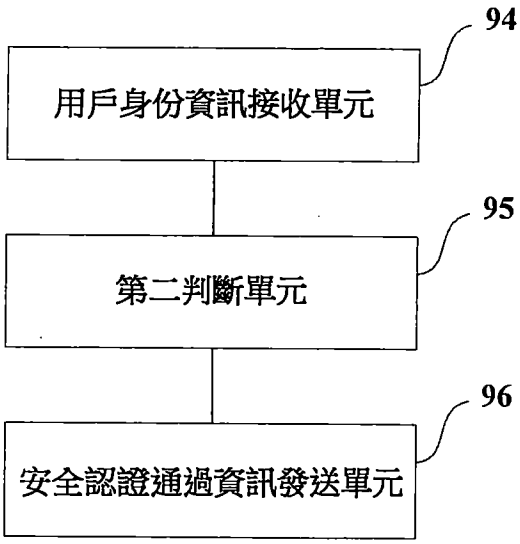
94
用戶身份資訊接收單元
95
第二判斷單元
96
安全認證通過資訊發送單元

圖 24

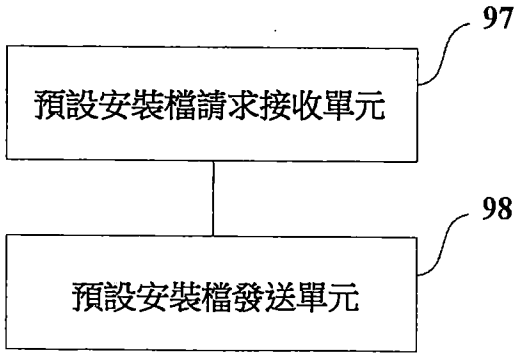
97
預設安裝檔請求接收單元
98
預設安裝檔發送單元

圖 25