I502524

(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 I502524 B**

(45)公告日： 中華民國 104 (2015) 年 10 月 01 日

(21)申請案號：099106472 (22)申請日： 中華民國 99 (2010) 年 03 月 05 日

(51)Int. Cl.： *G06Q20/00 (2012.01)*

(71)申請人：阿里巴巴集團控股有限公司 (開曼群島) ALIBABA GROUP HOLDING LIMITED (KY)

香港

(72)發明人：王瑞華 (CN)

(74)代理人：林志剛

(56)參考文獻：

TW	200943887A	US	5978840
US	2002/0046189A1	US	2007/0255652A1
US	2008/0048025A1		

審查人員：莊東燐

申請專利範圍項數：13 項 圖式數：10 共 42 頁

(54)名稱

支付資料處理方法、系統、支付終端及支付伺服器

(57)摘要

本案實施例揭示了支付資料處理方法、系統、支付終端及支付伺服器，該方法包括：接收方終端向給付方終端發送接收方資訊；接收方終端接收給付方終端返回的加密後的支付請求資料，並將加密後的支付請求資料和支付金額轉發至支付伺服器；接收方終端接收該支付伺服器驗證該加密後的支付請求資料和支付金額，並根據驗證結果執行支付後，返回的加密後的支付結果資料；接收方終端將該加密後的支付結果資料返回該給付方終端。本案實施例提高了支付資料在傳輸過程中的安全性和可靠性，同時也保證了支付方的個人資訊的安全性；由於給付方用戶可以在自己的私有設備上驗證支付金額，輸入密碼資訊，因此增強了支付體驗。

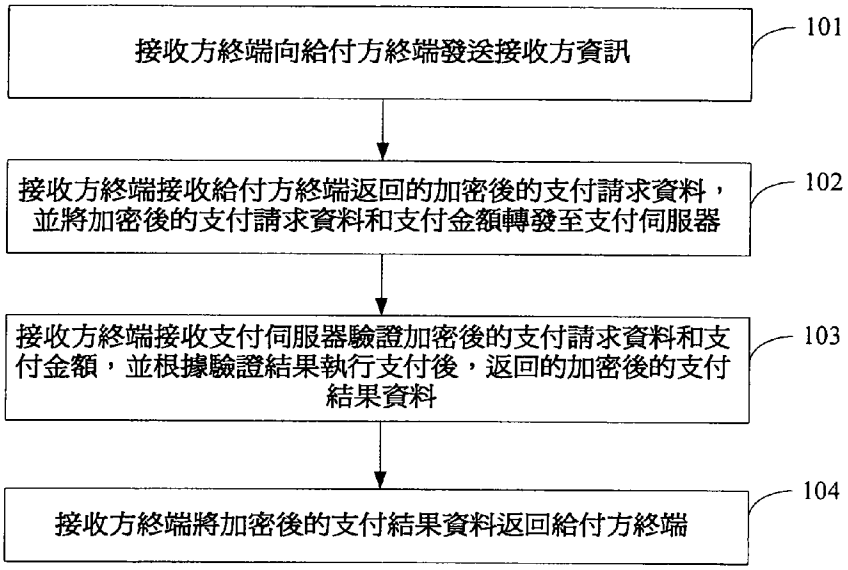
接收方終端向給付方終端發送接收方資訊
101
接收方終端接收給付方終端返回的加密後的支付請求資料，並將加密後的支付請求資料和支付金額轉發至支付伺服器
102
接收方終端接收支付伺服器驗證加密後的支付請求資料和支付金額，並根據驗證結果執行支付後，返回的加密後的支付結果資料
103
接收方終端將加密後的支付結果資料返回給付方終端
104

圖1

861444

發明專利說明書

公告本

（本申請書格式、順序，請勿任意更動，※記號部分請勿填寫）

※申請案號：99106472

※申請日：99 年 03 月 05 日　　※IPC 分類：G06Q 20/00 (2012.01)

一、發明名稱：（中文／英文）

支付資料處理方法、系統、支付終端及支付伺服器

二、中文發明摘要：

本案實施例揭示了支付資料處理方法、系統、支付終端及支付伺服器，該方法包括：接收方終端向給付方終端發送接收方資訊；接收方終端接收給付方終端返回的加密後的支付請求資料，並將加密後的支付請求資料和支付金額轉發至支付伺服器；接收方終端接收該支付伺服器驗證該加密後的支付請求資料和支付金額，並根據驗證結果執行支付後，返回的加密後的支付結果資料；接收方終端將該加密後的支付結果資料返回該給付方終端。本案實施例提高了支付資料在傳輸過程中的安全性和可靠性，同時也保證了支付方的個人資訊的安全性；由於給付方用戶可以在自己的私有設備上驗證支付金額，輸入密碼資訊，因此增強了支付體驗。

三、英文發明摘要：

四、指定代表圖：

（一）本案指定代表圖為：第（1）圖。

（二）本代表圖之元件符號簡單說明：無

五、本案若有化學式時，請揭示最能顯示發明特徵的化學式：無

六、發明說明：

【發明所屬之技術領域】

本案關於通信技術領域，尤其關於支付資料處理方法、系統、支付終端及支付伺服器。

【先前技術】

如今電子支付已成爲人們日常生活中廣泛使用的支付方式，電子支付指單位或個人透過電子終端，直接或間接向銀行等金融機構發出支付指令，實現貨幣支付與資金轉移的過程。一種常見的電子支付方式爲銷售點終端支付（例如，在商場購買商品），這種支付方式需要用戶隨身攜帶銀行卡，銷售方設置有與銀行聯網的刷卡機，當用戶購買商品時，銷售方透過刷卡機完成支付，從用戶的銀行帳戶中轉帳相應的金額到銷售方的銀行帳戶中。

隨著手機、PDA 等行動終端的普及，業界出現了透過手機及 PDA 等行動終端代替銀行卡來完成上述銷售點支付的方式，這種支付方式又被稱爲行動支付，但上述行動支付方式需要在手機中加裝智慧晶片或者改裝現有的 SIM 卡，且銷售點也需要對應安裝特定的裝置來配合使用，這些晶片及裝置本身的價值不菲，安裝也較爲複雜，由此造成銷售方及消費者使用該種支付方式的成本上升，導致行動支付難以普及，降低了用戶的支付體驗；並且，上述行動支付方式中支付資料在傳輸過程中由於缺少安全保證措施，相應降低了行動支付的安全性。

【發明內容】

本案實施例的目的是提供支付資料處理方法、系統、支付終端及支付伺服器，以提高用戶在行動支付過程中的支付體驗和支付安全性。

爲解決上述技術問題，本案實施例提供了一種支付資料處理方法，是這樣實現的：

一種支付資料處理方法，包括：

接收方終端向給付方終端發送接收方資訊；

接收方終端接收該給付方終端返回的加密後的支付請求資料，並將該加密後的支付請求資料和支付金額轉發至支付伺服器，該支付請求資料包括給付方資訊、接收方資訊和支付金額；

接收方終端接收該支付伺服器驗證該加密後的支付請求資料和支付金額，並根據驗證結果執行支付後，返回的加密後的支付結果資料；

接收方終端將該加密後的支付結果資料返回該給付方終端。

爲解決上述技術問題，本案實施例還提供了一種支付資料處理方法，是這樣實現的：

一種支付資料處理方法，包括：

支付伺服器接收接收方終端發送的加密後的支付請求資料和支付金額，該支付請求資料爲該給付方終端接收該接收方終端發送的接收方資訊後返回的支付請求資料，該支付請求資料包括給付方資訊、接收方資訊和支付金額；

支付伺服器驗證該加密後的支付請求資料和支付金額，並根據驗證結果執行支付；

支付伺服器向該接收方終端返回加密後的支付結果資料。

爲解決上述技術問題，本案實施例還提供了一種支付資料處理方法，是這樣實現的：

一種支付資料處理方法，包括：

給付方終端接收接收方終端發送的接收方資訊；

給付方終端向該接收方終端返回加密後的支付請求資料，該支付請求資料包括給付方資訊、接收方資訊和支付金額，該支付請求資料用於當該接收方終端將該加密後的支付請求資料和支付金額轉發至支付伺服器後，由該支付伺服器驗證該加密後的支付請求資料和支付金額，根據驗證結果執行支付並產生加密後的支付結果資料；

給付方終端接收該加密後的支付結果資料。

爲解決上述技術問題，本案實施例還提供了一種支付資料處理系統，是這樣實現的：

一種支付資料處理系統，包括：給付方終端、接收方終端和支付伺服器；

該給付方終端，用於接收到接收方終端發送的接收方資訊後，向該接收方終端返回加密後的支付請求資料，該支付請求資料包括給付方資訊、接收方資訊和支付金額；

該接收方終端，用於將該加密後的支付請求資料和支付金額轉發至支付伺服器；

該支付伺服器，用於驗證該加密後的支付請求資料和支付金額，並根據驗證結果執行支付，向該接收方終端返回加密後的支付結果資料；

該接收方終端，還用於將該加密後的支付結果資料返回該給付方終端。

爲解決上述技術問題，本案實施例還提供了一種支付終端，是這樣實現的：

一種支付終端，包括：

發送單元，用於向給付方終端發送接收方資訊；

轉發單元，用於接收該給付方終端返回的加密後的支付請求資料，並將該加密後的支付請求資料和支付金額轉發至支付伺服器，該支付請求資料包括給付方資訊、接收方資訊和支付金額；

接收單元，用於接收該支付伺服器驗證該加密後的支付請求資料和支付金額，並根據驗證結果執行支付後，返回的加密後的支付結果資料；

返回單元，用於將該加密後的支付結果資料返回該給付方終端。

爲解決上述技術問題，本案實施例還提供了一種支付伺服器，是這樣實現的：

一種支付伺服器，包括：

接收單元，用於接收接收方終端發送的加密後的支付請求資料和支付金額，該支付請求資料爲該給付方終端接收該接收方終端發送的接收方資訊後返回的支付請求資料

，該支付請求資料包括給付方資訊、接收方資訊和支付金額；

驗證單元，用於驗證該加密後的支付請求資料和支付金額，並根據驗證結果執行支付；

返回單元，用於向該接收方終端返回加密後的支付結果資料。

爲解決上述技術問題，本案實施例還提供了一種支付終端，是這樣實現的：

一種支付終端，包括：

接收單元，用於接收接收方終端發送的接收方資訊；

返回單元，用於向該接收方終端返回加密後的支付請求資料，該支付請求資料包括給付方資訊、接收方資訊和支付金額，該支付請求資料用於當該接收方終端將該加密後的支付請求資料和支付金額轉發至支付伺服器後，由該支付伺服器驗證該加密後的支付請求資料和支付金額，根據驗證結果執行支付並產生加密後的支付結果資料；

該接收單元，還用於接收該加密後的支付結果資料。

可見，在本案實施例中，給付方終端接收到接收方終端發送的接收方資訊後，向接收方終端返回加密後的支付請求資料，接收方終端將加密後的支付請求資料和支付金額轉發至支付伺服器，該支付伺服器驗證加密後的支付請求資料和支付金額，並根據驗證結果執行支付後，向接收方終端返回加密後的支付結果資料，接收方終端將加密後的支付結果資料返回給付方終端，從而完成安全支付過程

。本案實施例在支付資料處理過程中，由給付方終端和支付伺服器對支付資料進行獨立于接收方終端的加密處理，由此提高了支付資料在傳輸過程中的安全性和可靠性，同時也保證了支付方的個人資訊的安全性；本案實施例可應用在面對面的支付場景下，終端無需進行硬體上的改進，例如兩台手機之間也可以透過支付伺服器實現給付方終端的安全支付，因此提高了給付方終端持有者的支付體驗。

【實施方式】

本案實施例提供了支付資料處理方法、系統、支付終端及支付伺服器。

本案實施例中，關於給付方終端、接收方終端和支付伺服器。支付伺服器可以爲透過網路或專線與銀行相連並具備信譽保障的獨立于給付方和接收方的第三方機構提供的支付平臺，例如，支付寶（www.alipay.com）；給付方終端和接收方終端均可以是手機、PDA（Personal Digital Assistant，個人數碼助理）、筆記本電腦等便於隨身攜帶的電子終端。其中，給付方終端和接收方終端內預先設置了由支付伺服器方提供的用於進行支付資料處理的用戶端軟體，給付方終端僅與接收方終端透過終端設備連通交互，接收方終端透過網路與支付伺服器連通，由此買家利用商家的網路進行安全快速的電子支付。

爲了使本技術領域的人員更好地理解本案中的技術方案，下面將結合本案實施例中的附圖，對本案實施例中的

技術方案進行清楚、完整地描述，顯然，所描述的實施例僅僅是本案一部分實施例，而不是全部的實施例。基於本案中的實施例，本領域普通技術人員在沒有作出創造性勞動前提下所獲得的所有其他實施例，都應當屬於本案保護的範圍。

本案支付資料處理方法的第一實施例流程如圖 1 所示，該實施例從接收方終端側描述了支付資料處理過程：

步驟 101：接收方終端向給付方終端發送接收方資訊。

本案實施例中，給付方終端內安裝了由支付伺服器方提供的用於進行支付的電子支付軟體（用戶端軟體），接收方終端安裝了由支付伺服器方提供的用於進行收款的電子收款軟體（用戶端軟體）。其中，接收方終端和支付伺服器之間可以透過網際網路、無線網路或者其他專有網路進行通訊，而給付方終端不直接與支付伺服器通訊。給付方終端和接收方終端雙方均預先在支付伺服器上設置了支付帳號，分別爲給付方帳號和接收方帳號，同時支付伺服器還要保存給付方終端的支付密碼。

開始本次支付後，給付方終端和接收方終端之間可以透過有線方式相連，例如，給付方終端爲手機，接收方終端爲一台電腦，則二者可以透過 mini-usb 線連接；給付方終端和接收方終端之間也可以透過無線方式相連，例如，透過藍牙、紅外、wifi 等方式相連。

接收方終端和支付伺服器之間有一個同步的支付序列

號，用於唯一標識每一次支付。該支付序列號可以是在每一次支付開始時，由支付伺服器向接收方終端分配的亂數，也可以是支付伺服器與接收方終端之間相互約定一個演算法，從某個約定的數開始，每次支付成功後該數加 1，將該數作爲支付序列號。

接收方終端向給付方終端發送的接收方資訊中，包含了接收方帳號和支付伺服器爲接收方終端提供的支付序列號，另外，也可以包含接收方終端確認的支付金額。

步驟 102：接收方終端接收給付方終端返回的加密後的支付請求資料，並將加密後的支付請求資料和支付金額轉發至支付伺服器。

爲了保證給付方終端與支付伺服器之間透過接收方終端實現安全可靠的電子支付，給付方終端和支付伺服器之間預先約定了加密演算法，接收方終端無法得知該加密演算法或者破解該加密演算法，也就是保證了給付方終端和支付伺服器之間傳輸支付資料的安全性。例如，可以採用 RSA 加密演算法，支付伺服器知道自己的私鑰，並揭示自己的公鑰，給付方終端透過公鑰加密支付請求資料，由於接收方終端或者其他第三方不知道支付伺服器的私鑰，因此無法破解或者僞造該支付請求資料。

給付方終端接收到接收方資訊後，獲取其中的接收方帳號和支付序列號，給付方終端同時需要輸入支付密碼，然後給付方終端將給付方帳號、支付密碼、支付序列號、接收方帳號和支付金額按照約定的加密演算法進行加密。

需要說明的是，如果在步驟 101 中，當該接收方終端向給付方終端發送支付金額時，則給付方終端返回的加密後的支付請求資料中包含的支付金額即爲接收方終端發送的支付金額，接收方終端將加密後的支付請求資料及支付金額轉發至支付伺服器；當接收方終端未向給付方終端發送支付金額時，給付方終端返回的加密後的支付請求資料中包含的支付金額爲給付方終端輸入的支付金額，接收方終端接收給付方終端返回的加密後的支付請求資料及給付方終端輸入的支付金額，此時接收方終端可以首先驗證該支付金額是否正確，確認後接收方終端再將加密後的支付請求資料及支付金額轉發至支付伺服器。

步驟 103：接收方終端接收支付伺服器驗證加密後的支付請求資料和支付金額，並根據驗證結果執行支付後，返回的加密後的支付結果資料。

支付伺服器接收到接收方終端轉發的加密後的支付請求資料和支付金額後，按照預先約定的加密演算法，對加密後的支付請求資料進行解密，獲取解密後的給付方帳號、支付密碼、接收方帳號、支付序列號和支付金額，支付伺服器分別判斷上述解密後的給付方帳號、支付密碼、接收方帳號和支付序列號與預先保存的給付方帳號、支付密碼、接收方帳號和支付序列號是否一致，以及解密後的支付金額與該接收的支付金額是否一致，若所有資料均一致，則根據支付金額執行支付，並產生支付成功的支付結果資料，否則只要有一項資料不一致，就取消執行支付。

如果支付成功，則相應產生支付成功的支付結果描述，如果支付取消，則相應產生支付失敗的支付結果描述。同時支付伺服器對支付結果描述、支付完成時間、給付方帳號、接收方帳號、支付金額和收款序列號按照預先約定的加密演算法進行加密產生加密後的支付結果資料，將加密後的支付結果資料發送到接收方終端。

步驟 104：接收方終端將加密後的支付結果資料返回給付方終端，結束當前流程。

本案支付資料處理方法的第二實施例流程如圖 2 所示，該實施例從支付伺服器側描述了支付資料處理過程：

步驟 201：支付伺服器接收接收方終端發送的加密後的支付請求資料和支付金額。

開始本次支付後，給付方終端和接收方終端之間可以透過有線方式或者無線方式相連，接收方終端和支付伺服器之間可以透過網際網路或者其他專有網路進行通訊，而給付方終端不直接與支付伺服器通訊。給付方終端和接收方終端雙方均預先在支付伺服器上設置了支付帳號，分別爲給付方帳號和接收方帳號，同時支付伺服器還要保存給付方終端的支付密碼。接收方終端和支付伺服器之間還有一個同步的支付序列號，用於唯一標識每一次支付。

接收方終端向給付方終端發送包含了接收方帳號和支付伺服器爲接收方終端提供的支付序列號，另外，接收方資訊中也可以包含接收方終端確認的支付金額。爲了保證給付方終端與支付伺服器之間透過接收方終端實現安全可

靠的電子支付，給付方終端和支付伺服器之間預先約定了加密演算法，給付方終端接收到接收方資訊後，獲取其中的接收方帳號和支付序列號，給付方終端同時需要輸入支付密碼，然後給付方終端將給付方帳號、支付密碼、支付序列號、接收方帳號和支付金額按照約定的加密演算法進行加密產生加密後的支付請求資料，並將該加密後的支付請求資料發送到接收方終端，由接收方終端將該加密後的支付請求資料和支付金額轉發到支付伺服器。

步驟 202：支付伺服器驗證加密後的支付請求資料和支付金額，並根據驗證結果執行支付。

支付伺服器接收到接收方終端轉發的加密後的支付請求資料和支付金額後，按照預先約定的加密演算法，對加密後的支付請求資料進行解密，獲取解密後的給付方帳號、支付密碼、接收方帳號、支付序列號和支付金額，支付伺服器分別判斷上述解密後的給付方帳號、支付密碼、接收方帳號和支付序列號與預先保存的給付方帳號、支付密碼、接收方帳號和支付序列號是否一致，以及解密後的支付金額與該接收的支付金額是否一致，若所有資料均一致，則根據支付金額執行支付，並產生支付成功的支付結果資料，否則只要有一項資料不一致，就取消執行支付。

步驟 203：支付伺服器向接收方終端返回加密後的支付結果資料，結束當前流程。

如果支付成功，則相應產生支付成功的支付結果描述，如果支付取消，則相應產生支付失敗的支付結果描述。

同時支付伺服器對支付結果描述、支付完成時間、給付方帳號、接收方帳號、支付金額和收款序列號按照預先約定的加密演算法進行加密產生加密後的支付結果資料，將加密後的支付結果資料發送到接收方終端。

本案支付資料處理方法的第三實施例流程如圖 3 所示，該實施例從給付方終端側描述了支付資料處理過程：

步驟 301：給付方終端接收接收方終端發送的接收方資訊。

開始本次支付後，給付方終端和接收方終端之間可以透過有線方式相連，例如，給付方終端爲手機，接收方終端爲一台電腦，則二者可以透過 mini-usb 線連接；給付方終端和接收方終端之間也可以透過無線方式相連，例如，透過藍牙、紅外、wifi 等方式相連。

接收方終端向給付方終端發送的接收方資訊中，包含了接收方帳號和支付伺服器爲接收方終端提供的支付序列號，另外，也可以包含接收方終端確認的支付金額。

步驟 302：給付方終端向接收方終端返回加密後的支付請求資料。

支付請求資料包括給付方資訊、接收方資訊和支付金額，該支付請求資料用於當接收方終端將加密後的支付請求資料和支付金額轉發至支付伺服器後，由支付伺服器驗證加密後的支付請求資料和支付金額，根據驗證結果執行支付並產生加密後的支付結果資料。

步驟 303：給付方終端接收加密後的支付結果資料，

結束當前流程。

其中，給付方終端可以接收由支付伺服器直接返回的加密後的支付結果資料，例如，如果給付方終端開通與支付伺服器的無線網路連接後，該支付結果資料可以透過無線網路進行傳輸；或者給付方終端也可以接收支付伺服器向接收方終端返回加密後的支付結果資料後，由接收方終端轉發的該加密後的支付結果資料，例如，如果僅僅接收方終端開通與支付伺服器的無線網路連接，而接收方終端與給付方終端透過無線或有線方式連接，則給支付結果資料由接收方終端轉發。

上述從給付方終端側描述的支付資料處理過程的實施例與前述從接收方終端側描述的支付處理過程的實施例相比，其具體實現過程類似，因此對每個步驟不再贅述，可參見前述實施例的描述。

本案支付資料處理方法的第四實施例流程如圖 4 所示，該實施例從給付方終端、接收方終端和支付伺服器三方交互描述了支付資料的處理過程：

步驟 401：支付伺服器內預先儲存給付方終端的給付方帳號和支付密碼，以及接收方終端的接收方帳號。

支付伺服器是由支付提供商維護的伺服器，給付方終端和接收方終端作爲給付方和接收方分別在該支付提供商處開有帳戶，由支付伺服器保存給付方終端的給付方帳號和支付密碼，以及接收方終端的接收方帳號。

同時，給付方終端內安裝了由支付伺服器方提供的用

於進行支付的電子支付軟體（用戶端軟體），接收方終端安裝了由支付伺服器方提供的用於進行收款的電子收款軟體（用戶端軟體）。其中，接收方終端和支付伺服器之間可以透過網際網路或者其他專有網路進行通訊，而給付方終端不直接與支付伺服器通訊。

給付方終端和接收方終端可以爲手機、電腦等電子設備，並且接收方終端可以不局限於一台電子設備。

步驟 402：給付方終端和支付伺服器之間預先約定加密演算法並保存。

給付方終端和支付伺服器之間預先約定了加密演算法，接收方終端無法得知該加密演算法或者破解該加密演算法，也就是保證了給付方終端和支付伺服器之間傳輸支付資料的安全性。例如，可以採用 RSA 加密演算法，支付伺服器知道自己的私鑰，並揭示自己的公鑰，給付方終端透過公鑰加密支付請求資料，由於接收方終端或者其他第三方不知道支付伺服器的私鑰，因此無法破解或者僞造該支付請求資料。

另外，本案實施例中可以使用現有的各種加密演算法，其中可以採用一種加密演算法，也可以採用幾種加密演算法的組合，當採用加密演算法的組合時，給付方終端可以在傳輸支付請求資料時，同時傳輸加密演算法的類型。

由於本案實施例中，給付方終端和支付伺服器之間透過接收方終端傳輸加密後的支付資料，因此上方預先約定的加密演算法主要用於保證接收方終端無法破解或者僞造

，即加密後的支付資料接收方終端無法篡改或者無法猜測使用了何種演算法，從而無法破解和僞造。

步驟 403：本次支付開始，接收方終端和給付方終端之間連通。

開始本次支付後，給付方終端和接收方終端之間可以透過有線方式相連，例如，給付方終端爲手機，接收方終端爲一台電腦，則二者可以透過 mini-usb 線連接；給付方終端和接收方終端之間也可以透過無線方式相連，例如，透過藍牙、紅外、wifi 等方式相連。

另外，給付方終端和接收方終端之間也可以採用儲存卡、硬碟等資料中轉設備進行通信。

步驟 404：支付伺服器向接收方終端提供唯一標識本次支付的支付序列號並保存該支付序列號。

接收方終端和支付伺服器之間有一個同步的支付序列號，用於唯一標識每一次支付。該支付序列號可以是在每一次支付開始時，由支付伺服器向接收方終端分配的亂數，也可以是支付伺服器與接收方終端之間相互約定一個演算法，從某個約定的數開始，每次支付成功後該數加 1，將該數作爲支付序列號。

步驟 405：接收方終端向給付方終端發送包含支付序列號和接收方帳號的接收方資訊。

接收方終端向給付方終端發送的接收方資訊中，包含了接收方帳號和支付伺服器爲接收方終端提供的支付序列號，另外，也可以包含接收方終端確認的支付金額。

步驟 406：給付方終端將給付方帳號、支付密碼、接收方帳號、支付序列號和支付金額透過加密演算法進行加密產生支付請求資料後，將支付請求資料和支付金額發送到接收方終端。

需要說明的是，如果在步驟 305 中，當該接收方終端向給付方終端發送支付金額時，則給付方終端返回的加密後的支付請求資料中包含的支付金額即爲接收方終端發送的支付金額；當接收方終端未向給付方終端發送支付金額時，給付方終端返回的加密後的支付請求資料中包含的支付金額爲給付方終端輸入的支付金額，接收方終端接收給付方終端返回的加密後的支付請求資料及給付方終端輸入的支付金額。

步驟 407：接收方終端驗證支付金額正確後，將支付請求資料和支付金額轉發到支付伺服器。

假設步驟 405 中，接收方終端未向給付方終端發送支付金額時，則給付方終端返回的加密後的支付請求資料中包含的支付金額爲給付方終端輸入的支付金額，接收方終端接收給付方終端返回的加密後的支付請求資料及給付方終端輸入的支付金額，此時接收方終端可以首先驗證該支付金額是否正確，確認後接收方終端再將加密後的支付請求資料及支付金額轉發至支付伺服器。

步驟 408：支付伺服器按照預先約定的加密演算法，對支付請求資料進行解密，獲取解密後的給付方帳號、支付密碼、接收方帳號、支付序列號和支付金額。

步驟 409：支付伺服器判斷解密後的支付資料是否與儲存的支付資料均一致，若是，則執行步驟 410；否則，執行步驟 416。

支付伺服器讀取儲存的給付方帳號、支付密碼、接收方帳號和支付序列號，然後分別比較讀取的給付方帳號與解密後的給付方帳號是否一致，讀取的支付密碼是否與解密後的支付密碼一致，讀取的接收方帳號與解密後的接收方帳號是否一致，以及讀取的支付序列號與解密後的支付序列號是否一致。

步驟 410：支付伺服器判斷解密後的支付金額與接收到的支付金額是否一致，若是，則執行步驟 411；否則，執行步驟 416。

如果步驟 309 中所比較的讀取的資料和解密後的資料均一致，則進一步比較解密後的支付金額與接收到的支付金額是否一致。

步驟 411：根據支付金額執行支付，並產生支付成功的支付結果資料。

如果支付成功，則相應產生支付成功的支付結果描述，如果支付取消，則相應產生支付失敗的支付結果描述。

步驟 412：支付伺服器透過加密演算法對支付結果資料進行加密產生加密後的支付結果資料。

支付伺服器對支付結果描述、支付完成時間、給付方帳號、接收方帳號、支付金額和收款序列號按照預先約定的加密演算法進行加密產生加密後的支付結果資料，將加

密後的支付結果資料發送到接收方終端。

在支付結果資料中加入支付完成時間的目的，在於進一步加強支付的安全性，這是因爲該支付結果資料是需要透過接收方終端轉發到給付方終端的，爲了避免接收方終端使用歷史資料進行僞造，支付完成時間作爲一個不可重復使用的亂數，可以使給付方終端辨識每一次支付是否安全。

步驟 413：支付伺服器將支付結果資料發送至接收方終端，並刪除本次支付的支付序列號。

步驟 414：接收方終端將加密後的支付結果資料返回給付方終端。

步驟 415：給付方終端解密支付結果資料，驗證支付結果資料的可信性並完成支付，結束當前流程。

步驟 416：取消執行支付，結束當前流程。

與本案支付資料處理方法的實施例相對應，本案還提供了支付資料處理系統、支付終端和支付伺服器的實施例。

參見圖 5，爲本案支付資料處理系統的實施例框圖。

該支付資料處理系統包括：給付方終端 510、接收方終端 520 和支付伺服器 530。

其中，該給付方終端 510，用於接收到接收方終端 520 發送的接收方資訊後，向該接收方終端 520 返回加密後的支付請求資料，該支付請求資料包括給付方資訊、接收方資訊和支付金額；

該接收方終端 520，用於將該加密後的支付請求資料和支付金額轉發至支付伺服器 530；

該支付伺服器 530，用於驗證該加密後的支付請求資料和支付金額，並根據驗證結果執行支付，向該接收方終端 520 返回加密後的支付結果資料；

該接收方終端 520，還用於將該加密後的支付結果資料返回該給付方終端 510。

參見圖 6，爲本案一種支付終端的第一實施例框圖，該支付終端在實際應用中可以爲支付資料處理過程中的接收方終端。

該支付終端包括：發送單元 610、轉發單元 620、接收單元 630 和返回單元 640。

其中，發送單元 610，用於向給付方終端發送接收方資訊；

轉發單元 620，用於接收該給付方終端返回的加密後的支付請求資料，並將該加密後的支付請求資料和支付金額轉發至支付伺服器，該支付請求資料包括給付方資訊、接收方資訊和支付金額；

接收單元 630，用於接收該支付伺服器驗證該加密後的支付請求資料和支付金額，並根據驗證結果執行支付後，返回的加密後的支付結果資料；

返回單元 640，用於將該加密後的支付結果資料返回該給付方終端。

參見圖 7，爲本案一種支付終端的第二實施例框圖，

該支付終端在實際應用中可以爲支付資料處理過程中的接收方終端。

該支付終端包括：連接單元 710、獲取單元 720、發送單元 730、轉發單元 740、接收單元 750 和返回單元 760。

其中，連接單元 710，用於開始支付時和該給付方終端之間連通，該連通的方式包括：採用藍牙、紅外、WIFI 的無線連通方式，或採用 USB 的有線連通方式；

獲取單元 720，用於接收該支付伺服器提供的唯一標識本次支付的支付序列號；

發送單元 730，用於向給付方終端發送包含支付序列號的接收方資訊；

轉發單元 740，用於接收該給付方終端返回的加密後的支付請求資料，並將該加密後的支付請求資料和支付金額轉發至支付伺服器，該支付請求資料包括給付方資訊、接收方資訊和支付金額；

接收單元 750，用於接收該支付伺服器驗證該加密後的支付請求資料和支付金額，並根據驗證結果執行支付後，返回的加密後的支付結果資料；

返回單元 760，用於將該加密後的支付結果資料返回該給付方終端。

參見圖 8，爲本案另一種支付終端的實施例框圖，該支付終端在實際應用中可以爲支付資料處理過程中的給付方終端。

該支付終端包括：接收單元 810 和返回終端 820。

其中，接收單元 810，用於接收接收方終端發送的接收方資訊；

返回單元 820，用於向該接收方終端返回加密後的支付請求資料，該支付請求資料包括給付方資訊、接收方資訊和支付金額，該支付請求資料用於當該接收方終端將該加密後的支付請求資料和支付金額轉發至支付伺服器後，由該支付伺服器驗證該加密後的支付請求資料和支付金額，根據驗證結果執行支付並產生加密後的支付結果資料；

該接收單元 810，還用於接收該加密後的支付結果資料。

其中，該接收單元 810 可以接收該支付伺服器直接返回的加密後的支付結果資料；或者，該接收單元 810 也可以接收該支付伺服器向該接收方終端返回加密後的支付結果資料後，由該接收方終端轉發的該加密後的支付結果資料。

參見圖 9，爲本案支付伺服器的第一實施例框圖。

該支付伺服器包括：接收單元 910、驗證單元 920 和返回單元 930。

其中，接收單元 910，用於接收接收方終端發送的加密後的支付請求資料和支付金額，該支付請求資料爲該給付方終端接收該接收方終端發送的接收方資訊後返回的支付請求資料，該支付請求資料包括給付方資訊、接收方資訊和支付金額；

驗證單元 920，用於驗證該加密後的支付請求資料和支付金額，並根據驗證結果執行支付；

返回單元 930，用於向該接收方終端返回加密後的支付結果資料。

參見圖 10，爲本案支付伺服器的第二實施例框圖。

該支付伺服器包括：預設單元 1010，儲存單元 1020、提供單元 1030、接收單元 1040、驗證單元 1050、返回單元 1060 和刪除單元 1070。

其中，預設單元 1010，用於與給付方終端之間預先約定加密演算法；

儲存單元 1020，用於預先儲存接收方帳號、給付方帳號和支付密碼；

提供單元 1030，用於向接收方終端提供唯一標識本次支付的支付序列號並保存該支付序列號；

接收單元 1040，用於接收接收方終端發送的加密後的支付請求資料和支付金額，該支付請求資料爲該給付方終端接收該接收方終端發送的接收方資訊後返回的支付請求資料，該支付請求資料包括給付方資訊、接收方資訊和支付金額，其中，給付方終端透過該加密演算法對支付請求資料進行加密產生加密後的支付請求資料，該接收方資訊包括該支付序列號和接收方帳號，該給付方資訊包括給付方帳號和支付密碼；

驗證單元 1050，用於驗證該加密後的支付請求資料和支付金額，並根據驗證結果執行支付；

返回單元 1060，用於向該接收方終端返回加密後的支付結果資料，其中，透過該加密演算法對支付結果資料進行加密產生該加密後的支付結果資料；

刪除單元 1070，用於當該返回單元 860 向該接收方終端返回加密後的支付結果資料後，刪除該支付序列號，該加密後的支付結果資料包括標識支付是否成功的支付結果描述、給付方資訊、接收方資訊和支付金額。

具體的，驗證單元 1050 包括（圖 10 中未示出）：解密單元，用於按照該預先約定的加密演算法，對該加密後的支付請求資料進行解密，獲取解密後的給付方帳號、支付密碼、接收方帳號、支付序列號和支付金額；判斷單元，用於分別判斷該解密後的給付方帳號、支付密碼、接收方帳號和支付序列號與預先保存的給付方帳號、支付密碼、接收方帳號和支付序列號是否一致，以及該解密後的支付金額與該接收的支付金額是否一致；執行單元，用於當該判斷單元的判斷結果均一致時，根據該支付金額執行支付，並產生支付成功的支付結果資料；否則，取消執行支付。

透過以上的實施方式的描述可知，在本案實施例中，給付方終端接收到接收方終端發送的接收方資訊後，向接收方終端返回加密後的支付請求資料，接收方終端將加密後的支付請求資料和支付金額轉發至支付伺服器，該支付伺服器驗證加密後的支付請求資料和支付金額，並根據驗證結果執行支付後，向接收方終端返回加密後的支付結果

資料，接收方終端將加密後的支付結果資料返回給付方終端，從而完成安全支付過程。本案實施例在支付資料處理過程中，由給付方終端和支付伺服器對支付資料進行獨立于接收方終端的加密處理，由此提高了支付資料在傳輸過程中的安全性和可靠性，同時也保證了支付方的個人資訊的安全性；本案實施例可應用在面對面的支付場景下，終端無需進行硬體上的改進，例如兩台手機之間也可以透過支付伺服器實現給付方終端的安全支付，因此提高了給付方終端持有者的支付體驗。

透過以上的實施方式的描述可知，本領域的技術人員可以清楚地瞭解到本案可借助軟體加必需的通用硬體平臺的方式來實現。基於這樣的理解，本案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，該電腦軟體產品可以儲存在儲存媒體中，如ROM/RAM、磁碟、光碟等，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）執行本案各個實施例或者實施例的某些部分該的方法。

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，對於系統實施例而言，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。

本案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、手持設備或攜帶型設備

、平板型設備、多處理器系統、基於微處理器的系統、置頂盒、可編程的消費電子設備、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計算環境等等。

本案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。也可以在分散式計算環境中實踐本案，在這些分散式計算環境中，由透過通信網路而被連接的遠端處理設備來執行任務。在分散式計算環境中，程式模組可以位於包括儲存設備在內的本地和遠端電腦儲存媒體中。

雖然透過實施例描繪了本案，本領域普通技術人員知道，本案有許多變形和變化而不脫離本案的精神，希望所附的申請專利範圍包括這些變形和變化而不脫離本案的精神。

【圖式簡單說明】

爲了更清楚地說明本案實施例或現有技術中的技術方案，下面將對實施例或現有技術描述中所需要使用的附圖作簡單地介紹，顯而易見地，下面描述中的附圖僅僅是本案中記載的一些實施例，對於本領域普通技術人員來講，在不付出創造性勞動性的前提下，還可以根據這些附圖獲得其他的附圖。

圖 1 爲本案支付資料處理方法的第一實施例流程圖；

圖 2 爲本案支付資料處理方法的第二實施例流程圖；

圖 3 爲本案支付資料處理方法的第三實施例流程圖；

圖 4 爲本案支付資料處理方法的第四實施例流程圖；

圖 5 爲本案支付資料處理系統的實施例框圖；

圖 6 爲本案一種支付終端的第一實施例框圖；

圖 7 爲本案一種支付終端的第二實施例框圖；

圖 8 爲本案另一種支付終端的實施例框圖；

圖 9 爲本案支付伺服器的第一實施例框圖；

圖 10 爲本案支付伺服器的第二實施例框圖。

【主要元件符號說明】

510：給付方終端

520：接收方終端

530：支付伺服器

610：發送單元

620：轉發單元

630：接收單元

640：返回單元

710：連接單元

720：獲取單元

730：發送單元

740：轉發單元

750：接收單元

760：返回單元

810：接收單元

820：返回單元

910：接收單元

920：驗證單元

930：返回單元

1010：預設單元

1020：儲存單元

1030：提供單元

1040：接收單元

1050：驗證單元

1060：返回單元

1070：刪除單元

七、申請專利範圍：

1.一種支付資料處理方法，其特徵在於，包括：

接收方產生第一支付金額；

接收方終端向給付方終端發送接收方資訊，其中，該接收方資訊包括接收方帳號、第一支付金額及唯一標識本次支付的支付序列號；

接收方終端接收該給付方終端返回的加密後的支付請求資料，其中，該加密後的支付請求資料包括給付方資訊、接收方資訊和給付方終端輸入的第二支付金額，且其中，該加密後的支付請求資料採用在給付方終端和支付伺服器之間預先約定的加密演算法且包括支付完成時間；

比較該第一支付金額與該第二支付金額是否一致；以及

如果該第一支付金額與該第二支付金額一致，則：

將該加密後的支付請求資料和該接收方產生的支付金額轉發至該支付伺服器，

接收方終端接收該支付伺服器產生的加密後的支付結果資料，其中，該加密後的支付結果資料是該支付伺服器按照預先約定的加密演算法進行加密產生；以及

接收方終端將該加密後的支付結果資料返回該給付方終端。

2.根據申請專利範圍第 1 項所述的方法，還包括：接收該支付伺服器提供的該支付序列號。

3.根據申請專利範圍第 1 項所述的方法，其中，當該接收方終端向給付方終端發送該第一支付金額時，該給付方終端返回的加密後的支付請求資料中包含該第二支付金額，該接收方終端將該加密後的支付請求資料及該第二支付金額轉發至該支付伺服器；以及

當該接收方終端未向給付方終端發送該第一支付金額時，該給付方終端返回的該加密後的支付請求資料中包含該給付方終端輸入的該第二支付金額，該接收方終端接收該給付方終端返回的該加密後的支付請求資料及該第二支付金額，該接收方終端將該加密後的支付請求資料及該第二支付金額轉發至該支付伺服器。

4.一種支付資料處理方法，其特徵在於，包括：

支付伺服器預先約定加密演算法；

該支付伺服器接收接收方終端發送的加密後的支付請求資料和第一支付金額，其中，該加密後的支付請求資料為給付方終端接收該接收方終端發送的接收方資訊後返回的支付請求資料按照該預先約定的加密演算法被加密，該加密後的支付請求資料包括給付方資訊、接收方資訊和該給付方終端輸入的第二支付金額，其中，該接收方資訊包括支付序列號、該第一支付金額和接收方帳號，且其中，該給付方資訊包括給付方帳號和支付密碼；

支付伺服器驗證該加密後的支付請求資料和該第二支付金額，並根據驗證結果執行支付；以及

按照預先約定的加密演算法對支付結果資料進行加密

產生該加密後的支付結果資料，其中，該加密後的支付結果資料包括支付完成時間；

該支付伺服器向該接收方終端返回該加密後的支付結果資料。

5.根據申請專利範圍第 4 項所述的方法，其中，還包括：該支付伺服器預先儲存了接收方帳號、給付方帳號和支付密碼；以及

該支付伺服器向接收方終端提供唯一標識本次支付的支付序列號並保存該支付序列號。

6.根據申請專利範圍第 5 項所述的方法，其中，該支付伺服器驗證加密後的支付請求資料和該第二支付金額，並根據驗證結果執行支付包括：

支付伺服器按照該預先約定的加密演算法，對該加密後的支付請求資料進行解密，獲取解密後的給付方帳號、支付密碼、接收方帳號、支付序列號和該第二支付金額；

支付伺服器分別判斷該解密後的給付方帳號、支付密碼、接收方帳號和支付序列號與預先保存的給付方帳號、支付密碼、接收方帳號和支付序列號是否一致，以及該解密後的該第二支付金額與該接收的該第一支付金額是否一致；

若均一致，則根據該支付金額執行支付，並產生支付成功的支付結果資料；以及

否則，取消執行支付。

7.根據申請專利範圍第 5 項所述的方法，其中，該支

付伺服器向接收方終端返回加密後的支付結果資料後，還包括：刪除該支付序列號；

該加密後的支付結果資料包括：標識支付是否成功的支付結果描述、給付方資訊、接收方資訊和支付金額。

8.一種支付資料處理方法，其特徵在於，包括：

支付伺服器預先約定加密演算法；

給付方終端接收接收方終端發送的接收方資訊，其中，該接收方資訊包括接收方帳號、接收方產生的第一支付金額及唯一標識本次支付的支付序列號；

給付方終端向該接收方終端返回加密後的支付請求資料，該加密後的支付請求資料包括給付方資訊、接收方資訊和給付方終端輸入的第二支付金額，其中，該加密後的支付請求資料按照該預先約定的加密演算法被加密，用於當該接收方終端將該加密後的支付請求資料和該第二支付金額轉發至支付伺服器後，由該支付伺服器驗證該加密後的支付請求資料和該第二支付金額，根據驗證結果執行支付並產生加密後的支付結果資料，其中，該給付方資訊包括給付方帳號和支付密碼，且其中，該接收終端比較該第二支付金額與該第一支付金額；以及

如果該第二支付金額與該第一支付金額一致，則給付方終端接收該支付伺服器產生的加密後的支付結果資料，該加密後的支付結果資料指出支付是否成功，其中，該加密後的支付結果資料是該支付伺服器按照預先約定的加密演算法進行加密產生且包括支付完成時間。

9.根據申請專利範圍第 8 項所述的方法，其中，該給付方終端接收該加密後的支付結果資料包括：

給付方終端接收該支付伺服器直接返回的加密後的支付結果資料；或

給付方終端接收該支付伺服器向該接收方終端返回加密後的支付結果資料後，由該接收方終端轉發的該加密後的支付結果資料。

10.一種支付資料處理系統，其特徵在於，包括：給付方終端、接收方終端和支付伺服器；

該給付方終端，用於與支付伺服器之間預先約定加密演算法，且接收到接收方終端發送的接收方資訊後，向該接收方終端返回加密後的支付請求資料，該支付請求資料包括給付方資訊、接收方資訊和給付方終端輸入的第二支付金額，其中，該接收方資訊包括接收方帳號和唯一標識本次支付的支付序列號，且其中，該給付方資訊包括給付方帳號和支付密碼；

該接收方終端，用於產生第一支付金額作為第一支付金額，比較該第一支付金額該第二支付金額，且如果該第一支付金額與該第二支付金額一致，則將該加密後的支付請求資料和該第二支付金額轉發至支付伺服器；

該支付伺服器，用於按照預先約定的加密演算法對該支付請求資料進行加密產生該加密後的支付請求資料、對該支付結果資料進行加密產生該加密後的支付結果資料，以及驗證該加密後的支付請求資料和該第二支付金額，並

根據驗證結果執行支付，向該接收方終端返回該加密後的支付結果資料，其中該加密的支付結果包括支付完成時間；以及

該接收方終端，還用於將該加密後的支付結果資料返回該給付方終端。

11.一種支付終端，其特徵在於，包括：

發送單元，用於向給付方終端發送接收方資訊，其中，該接收方資訊包括接收方帳號、支付金額及唯一標識本次支付的支付序列號；

轉發單元，用於接收該給付方終端返回的加密後的支付請求資料，並將該加密後的支付請求資料和支付金額轉發至支付伺服器，其中，該加密後的支付請求資料包括給付方資訊、接收方資訊和第二支付金額；

接收單元，用於接收該支付伺服器產生的加密後的支付結果資料，其中，該加密後的支付結果資料指出支付伺服器的支付是否成功，且其中，該加密後的支付請求資料採用在給付方終端和支付伺服器之間預先約定的加密演算法，且包括支付完成時間；以及

返回單元，用於將該加密後的支付結果資料返回該給付方終端。

12.一種支付伺服器，其特徵在於，包括：

支付伺服器預先約定加密演算法；

接收單元，用於接收接收方終端發送的加密後的支付請求資料和接收方所產生的第一支付金額，其中，該加密

的支付請求資料為給付方終端接收該接收方終端發送的接收方資訊後返回的支付請求資料按照預先約定的加密演算法進行加密產生，該加密的支付請求資料包括給付方資訊、接收方資訊和第二支付金額，其中，該接收方資訊包括支付序列號、該支付金額和接收方帳號，且其中，該給付方資訊包括給付方帳號和支付密碼；

驗證單元，用於驗證該加密後的支付請求資料和該第二支付金額，並根據驗證結果執行支付；以及

返回單元，用於向該接收方終端返回加密後的支付結果資料，其中，該加密後的支付結果資料按照預先約定的加密演算法進行加密產生，且其中該加密後的支付結果包括支付完成時間。

13.一種給付終端，其特徵在於，包括：

支付伺服器預先約定加密演算法；

接收單元，用於接收接收方終端發送的接收方資訊，其中，該接收方資訊包括接收方帳號、接收方產生的第一支付金額及唯一標識本次支付的支付序列號；

返回單元，用於向該接收方終端返回加密後的支付請求資料，該加密後的支付請求資料按照該預先約定的加密演算法被加密，且包括給付方資訊、接收方資訊和給付方終端輸入的第二支付金額，其中，該給付方資訊包括給付方帳號和支付密碼，且其中，該接收終端比較該第二支付金額與第一支付金額，當該接收方終端將該加密後的支付請求資料和該第二支付金額轉發至支付伺服器後，由該支

付伺服器驗證該加密後的支付請求資料和第二支付金額，根據驗證結果執行支付並按照預先約定的加密演算法產生加密後的支付結果資料，其中，該加密後的支付結果資料包括支付完成時間；

該接收單元，還用於如果該第二支付金額與該接收方產生的支付金額一致，則接收該支付伺服器產生的加密後的支付結果資料。

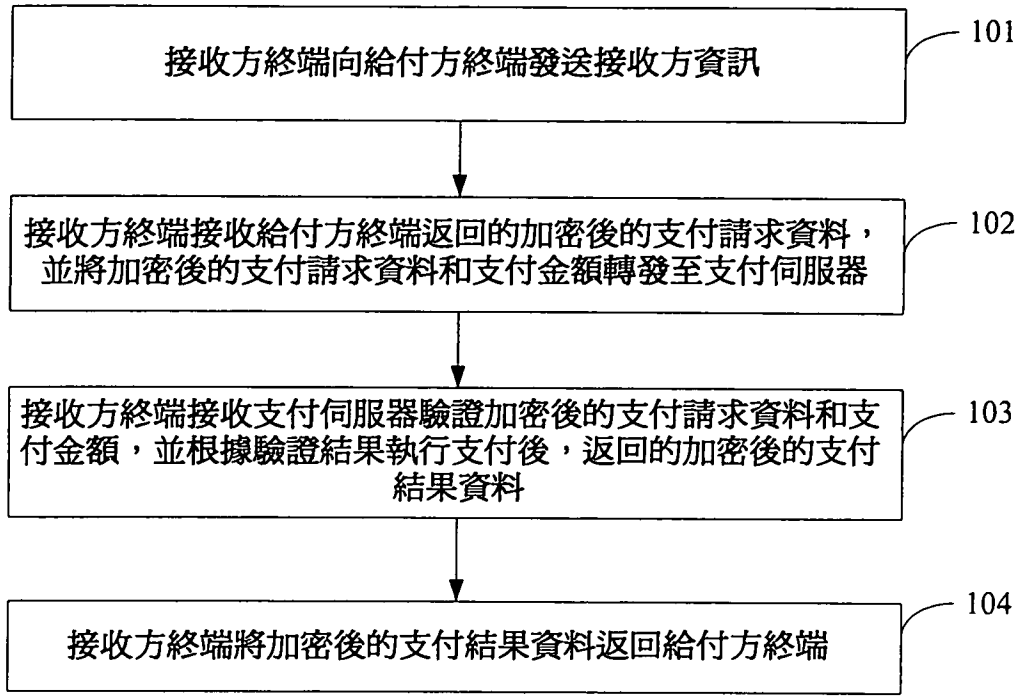
接收方終端向給付方終端發送接收方資訊
101
接收方終端接收給付方終端返回的加密後的支付請求資料，並將加密後的支付請求資料和支付金額轉發至支付伺服器
102
接收方終端接收支付伺服器驗證加密後的支付請求資料和支付金額，並根據驗證結果執行支付後，返回的加密後的支付結果資料
103
接收方終端將加密後的支付結果資料返回給付方終端
104

圖1

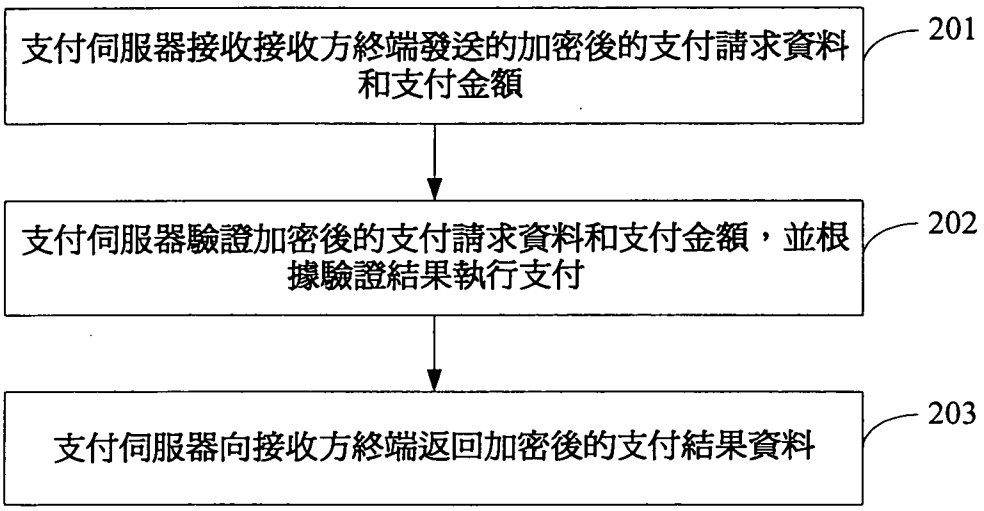
支付伺服器接收接收方終端發送的加密後的支付請求資料和支付金額
201
支付伺服器驗證加密後的支付請求資料和支付金額，並根據驗證結果執行支付
202
支付伺服器向接收方終端返回加密後的支付結果資料
203

圖2

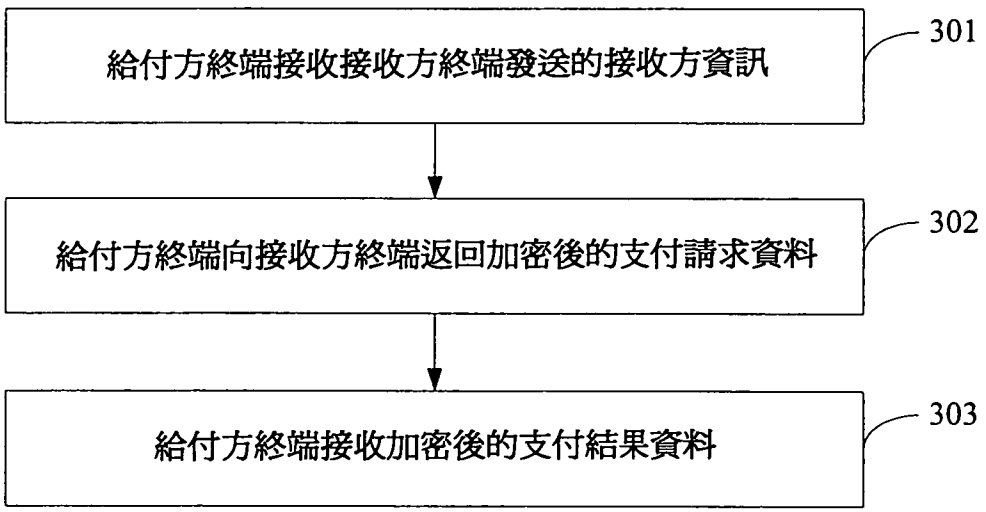
給付方終端接收接收方終端發送的接收方資訊
301
給付方終端向接收方終端返回加密後的支付請求資料
302
給付方終端接收加密後的支付結果資料
303

圖3

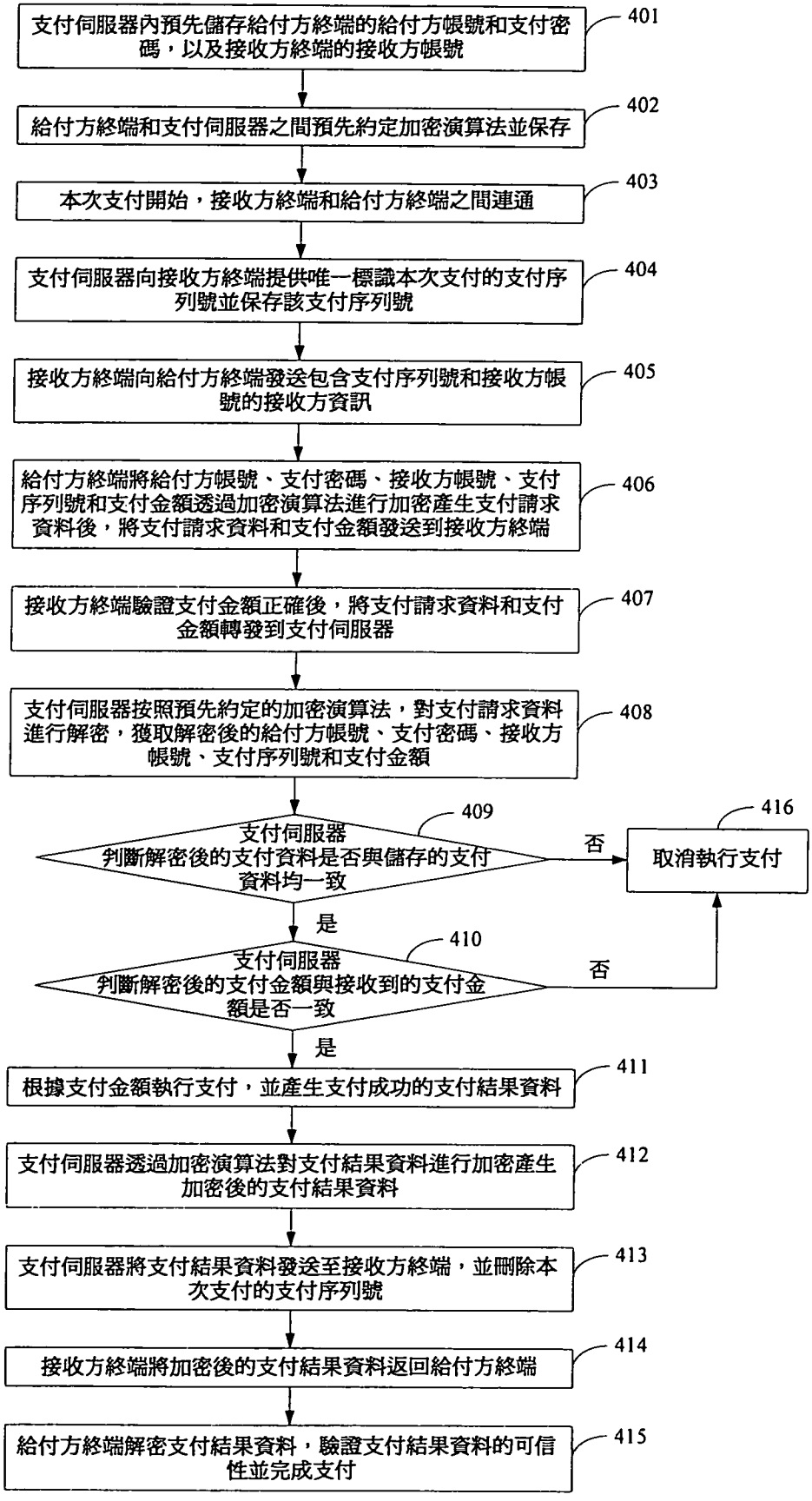
支付伺服器內預先儲存給付方終端的給付方帳號和支付密碼，以及接收方終端的接收方帳號
401
給付方終端和支付伺服器之間預先約定加密演算法並保存
402
本次支付開始，接收方終端和給付方終端之間連通
403
支付伺服器向接收方終端提供唯一標識本次支付的支付序列號並保存該支付序列號
404
接收方終端向給付方終端發送包含支付序列號和接收方帳號的接收方資訊
405
給付方終端將給付方帳號、支付密碼、接收方帳號、支付序列號和支付金額透過加密演算法進行加密產生支付請求資料後，將支付請求資料和支付金額發送到接收方終端
406
接收方終端驗證支付金額正確後，將支付請求資料和支付金額轉發到支付伺服器
407
支付伺服器按照預先約定的加密演算法，對支付請求資料進行解密，獲取解密後的給付方帳號、支付密碼、接收方帳號、支付序列號和支付金額
408
支付伺服器判斷解密後的支付資料是否與儲存的支付資料均一致
409
否
取消執行支付
416
是
支付伺服器判斷解密後的支付金額與接收到的支付金額是否一致
410
否
是
根據支付金額執行支付，並產生支付成功的支付結果資料
411
支付伺服器透過加密演算法對支付結果資料進行加密產生加密後的支付結果資料
412
支付伺服器將支付結果資料發送至接收方終端，並刪除本次支付的支付序列號
413
接收方終端將加密後的支付結果資料返回給付方終端
414
給付方終端解密支付結果資料，驗證支付結果資料的可信性並完成支付
415

圖4

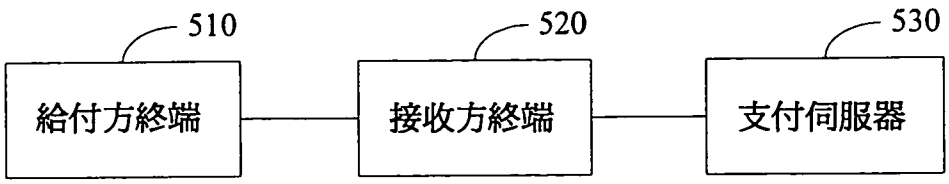
510
520
530
給付方終端
接收方終端
支付伺服器

圖5

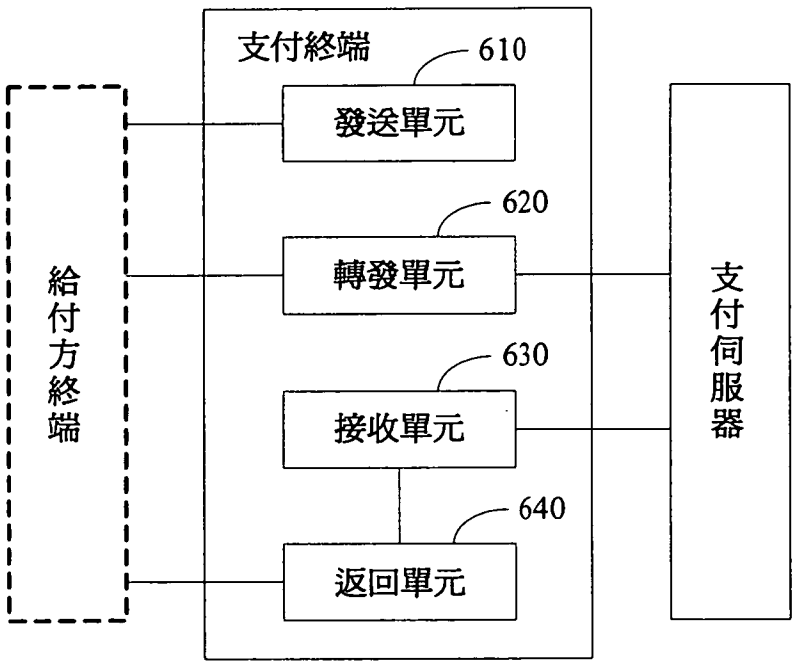
支付終端
610
發送單元
620
轉發單元
630
接收單元
640
返回單元
給付方終端
支付伺服器

圖6

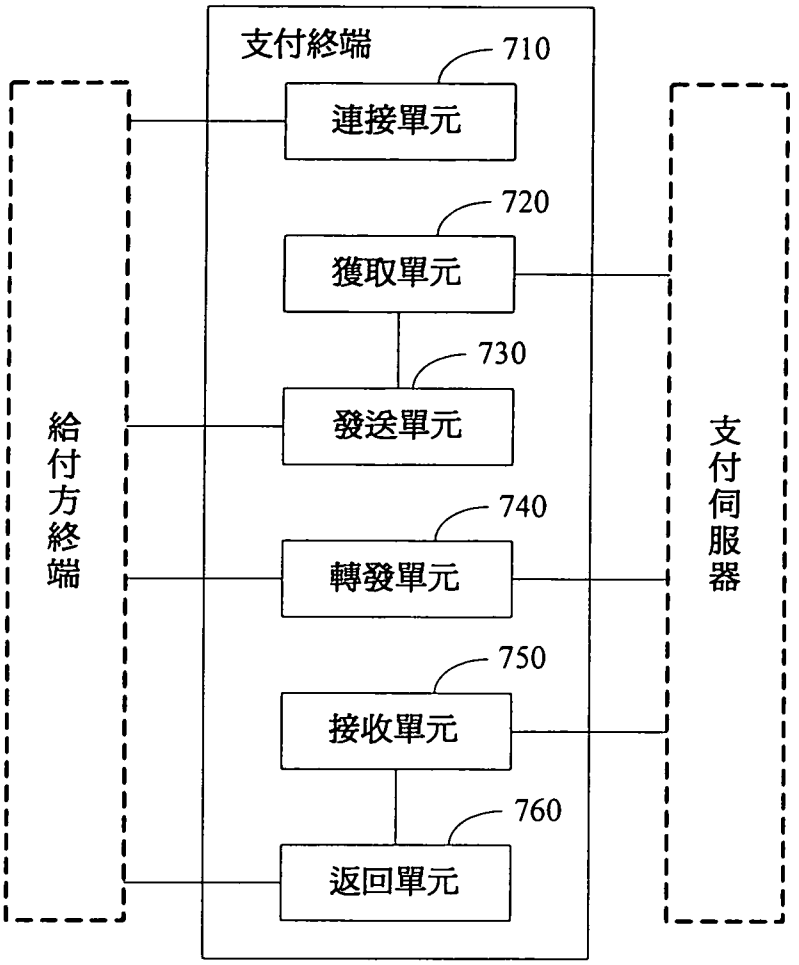
支付終端
710
連接單元
720
獲取單元
730
發送單元
740
轉發單元
750
接收單元
760
返回單元
給付方終端
支付伺服器

圖7

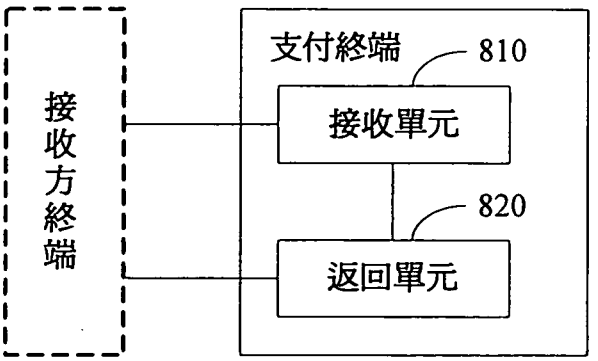
接收方終端
支付終端
810
接收單元
820
返回單元

圖8

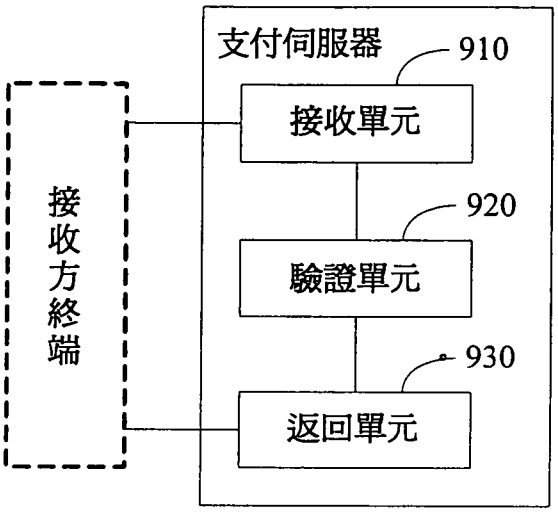
支付伺服器
910
接收單元
920
驗證單元
930
返回單元
接收方終端

圖9

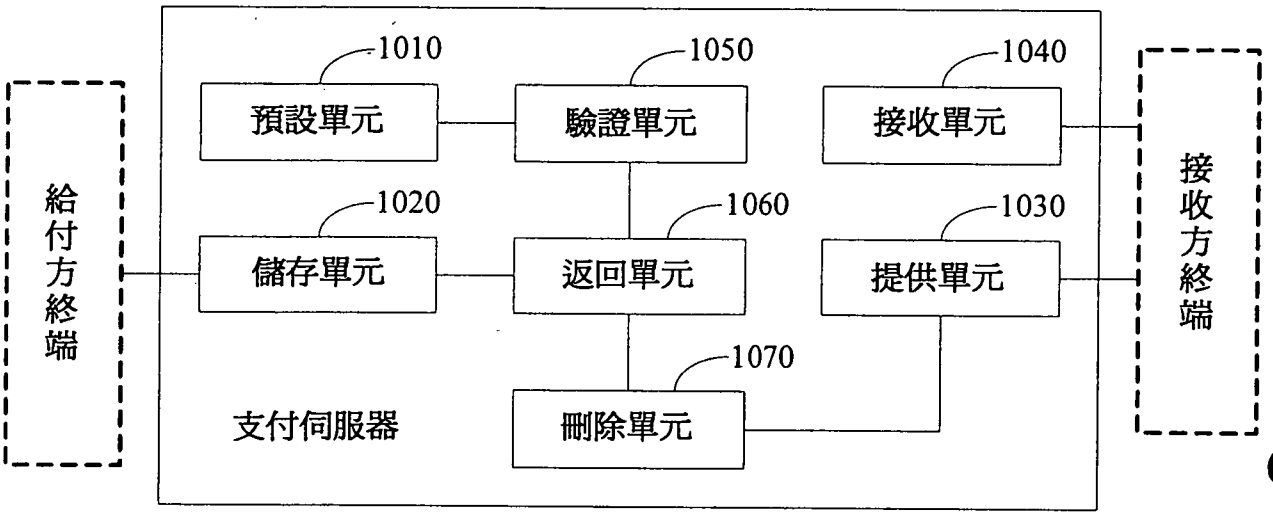
1010
預設單元
1050
驗證單元
1040
接收單元
給付方終端
1020
儲存單元
1060
返回單元
1030
提供單元
接收方終端
1070
支付伺服器
刪除單元

圖10