

申請日期	88.11.4
案 號	88119209
類 別	H04K1/00, H04L9/00

A4
C4

(以上各欄由本局填註)

發明
專利

專 利 說 明 書

476202

一、發明 名稱	中 文	電子交易用密碼系統與方法
	英 文	A CRYPTOGRAPHIC SYSTEM AND METHOD FOR ELECTRONIC TRANSACTIONS
二、發明 人	姓 名	傑伊 C. 陳
	國 籍	中華民國
	住、居所	美國加州聖馬利諾黑石路1355號
三、申請人	姓 名 (名稱)	傑伊 C. 陳
	國 籍	中華民國
	住、居所 (事務所)	美國加州聖馬利諾黑石路1355號
	代 表 人 姓 名	

經濟部智慧財產局員工消費合作社印製

裝

訂

線

承辦人代碼：	
大類：	
I P C分類：	

B6

美 國 (地 區) 申 請 專 利 , 申 請 日 期 : 案 號 : , ☐ 有 ☒ 無 主 張 優 先 權
1998.5.5 60/084,257

有關微生物已寄存於： _____，寄存日期： _____，寄存號碼： _____

(請先閱讀背面之注意事項再填寫本頁各欄)

裝

訂

線

五、發明說明(1)

發明領域

本發明乃執行安全電子交易之一種密碼系統與方法。更仔細而言是使用電子卡(electronic card)執行電子交易；電子卡是以智慧卡(smart card)形式，或是以具有智慧卡相等功能與實效之電腦軟體形式。

先前技術

積體電路卡片(integrated circuit card)有一個一般性的稱謂為智慧卡，即，一張信用卡尺寸大小之塑膠片上嵌有一個IC晶片。智慧卡上所嵌入之IC晶片中通常具有但卻又不是一定要包括下列之零件：中央微處理單元(CPU)、唯讀記憶體(Ready Only Memory)、隨機存取記憶體(Random Access Memory)、讀寫設備之輸入與輸出控制埠，以及一些持續性記憶體例如資料記錄區可利用電流自由重寫資料記憶體(EEPROM)。IC晶片能執行運算、邏輯處理、資料管理、通訊等工作。

智慧卡主要分成接觸式與非接觸式(遙感應式)兩種。國際標準組織(ISO)已將智慧卡訂定了一套ISO系列的相關標準，其中尤其ISO 7816標準是應用於各IC卡。正因為智慧卡具有執行運算之能力，智慧卡所可以支援多類的安全特色例如有：認證、安全讀與寫、對稱性金鑰及非對稱性金鑰之加密與解密等等。因此智慧卡是十分適合去擔當電子商務之中兩件最重要之任務，即、資料安全與認證。

智慧卡已在許多特定領域中被使用，例如：大眾捷運、健保、停車場、校園管理、加油站等等。智慧卡適用於

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明(2)

電子商務與其他金融領域之潛力，其受到歡迎的程度正以快步調增加中。一九九六年五月二十八日核發給羅伯·包爾(Robert S. Power)之美國專利號碼US5521362，其名稱為“電子錢包卡有複數個記憶體以防止不實使用暨對應之方法”，乃敘述有關智慧卡中電子錢包之運用，包爾之專利展示了智慧卡可以擔當安全金融工具之能力而不僅僅是一片儲存資料之裝置而已。

當科技使得智慧卡上之IC晶片運算速度與記憶體功能得以繼續提升時，多用途智慧卡之概念會將因成本變低後得以具體被實現。定名為“多用途數據卡”之美國專利號碼US5530232，於一九九六年六月二十五日核發給道格拉斯·泰勒(Douglas C. Taylor)，該專利是有關一片多用途數據卡，能去代替已有之單卡單用途，該發明並含及金融類卡與非金融類卡。多用途數據卡是用傳統之數據機連結方式將智慧卡與金融(或非金融)服務提供者相連結。泰勒的專利，“多用途數據卡”與任何種類開放型網路或是任何加密與解密方法均完全無關連。

定名為“適合複數服務提供者之智慧卡暨遠端裝置”之美國專利號碼US5544246，於一九九六年八月五日核發給曼德邦(Mandelbaum)等三人，該專利是讓多個金融(或非金融)服務提供者同時存在於一片智慧卡中，每一個服務提供者是智慧卡之使用人，每一個服務提供者均是被智慧卡製發人/所有權人所設定於智慧卡中。每一個智慧卡使用人均可建立一個樹枝狀的檔案並以不同的識別文字密碼

(請先閱讀背面之注意事項再填寫本頁)

訂

線

五、發明說明 (3)

組(通關密碼組)(password file)加以保護。曼德邦等三人之專利是敘述去新設定或去刪除智慧卡中之多重應用途徑，以適切但不相同的識別文字密碼去進入智慧卡中不同的應用途徑。

定名為“電子商務中一種安全導引系統”之美國專利號碼US5671279於一九九七年九月二十三日核發給塔爾·埃格默(Taher Elgamal)。是一個於開放型網路中使用非對稱性公開金鑰之電子商務系統。Elgamal之發明並沒有運用智慧卡為電子商務之工具，且所有參加電子交易者全是用電子憑證(digital certificates)(有另譯公鑰憑證)為相互間認證之工具。該系統、例如於網際網路上時，買方與賣方之間需要一個稱之為線上安全編碼傳輸(secure sockets layer, SSL)的安全系統。

定名為“電子商務中一種安全交易系統與方法”之美國專利號碼US5790677於一九九八年八月四日核發給芭芭拉·福斯(Barbara Fox)等五人。該專利是先用一個登錄程序之後再接續一個交易程序。於登錄程序之中，每一位交易參加者均向其所信任並已以要約拘束之電子憑證伺服器(trusted credential binding server)傳送一個登錄封包(packet)進行登錄。電子憑證伺服器是會根據所收到之信息，去製作一份獨一無二的電子憑證，並將此電子憑證傳送回給該位提出要求電子憑證者。於交易程序中，交易源始者，把其提出之要求信息傳送至不相同之接收者，所提出之要求包括商業文件與付款方法，交易源始者收到回覆

(請先閱讀背面之注意事項再填寫本頁)

裝 · 訂 · 線

五、發明說明(4)

信息並查驗所有不相同接收者之憑證內容，交易源始者用不相同之接收者的公開金鑰(public key)將商業文件與付款方法加密後傳送至不相同之接收者，如此不相同之接收者可以因而做解密，福斯之發明是安全電子交易標準(secure electronic transaction, SET)的主流，SET是目前美國幾家大型軟體公司與金融公司正在共同支持建立的一項以電子憑證為機制的電子商務系統。

定名為“提供安全電子通訊之裝置與方法”之美國專利號碼US5796840於一九九八年八月十八日核發給德瑞克·戴維思(Derek L. Davis)。該專利是一種半導體電子裝置能夠產生讓裝置專屬用之一對加密金鑰俾用於隨後的信息認證工作上。戴維思的半導體電子裝置是用非對稱性公開金鑰去確保通訊雙方身分的真實性。

定名為“免中央管控之安全化及個人化智慧卡系統與方法”之美國專利號碼US5534857於一九九六年七月九日核發給的賽門·梁(Simon G. Laing)及馬休·伯考克(Matthew P. Bowcock)。該專利敘述一種方法暨裝置如何安全地把隱私性資料由發訊端(issuer)寫入遠方收訊端之智慧卡上，一對儲存於安全電腦端(secure computer)與零售商智慧卡端(retailer smart card)上之共用金鑰(common key)用以產生一對(發訊端與收訊端)兩端共同所用之期間密鑰(session key)，該期間密鑰把往返於安全終端電腦系統(secure terminal)與安全電腦端間之數據進行加密及解密。

(請先閱讀背面之注意事項再填寫本頁)

訂

線

五、發明說明 (5)

以上所述及的先前技術其安全電子交易系統之結構都是涉及公開金鑰之基礎結構(public key infrastructure)，及其相關聯之電子憑證驗證中心(digital certificate authority, CA)。

開放型網路中，對稱性密秘金鑰密碼系統(secret key-based system)，其金鑰於大眾流通性與金鑰管理之靈活度兩方面是比較差，而也容易遭受電腦駭客的蓄意攻擊。而相較於另一方面，非對稱性公開金鑰密碼系統(public/private key-based system)固然有優於對稱性密秘金鑰密碼系統之處，但，非對稱性公開金鑰系統卻存有一項望之生畏的義務，那就是參加交易者人等相互間需要做身分之相互認證。本發明提出的系統與方法不需要使用憑證中心及電子憑證，本發明是一種以混合系統與方法為機制之電子交易。混合系統與方法於金鑰交換階段是使用非對稱性公開金鑰/私密金鑰，於交易階段是使用期間密鑰做為對稱性私秘金鑰/私秘金鑰。

本發明之結論

本發明是使用電子卡(electronic card, EC)執行電子交易之一種加密與解密系統與方法，電子卡是以智慧卡之形式或是以具有智慧卡相等功能之軟體去與網路做通聯(communicate)。

本發明較佳具體例方案是用網路，例如網際網路(Internet)，本發明另一個具體例是用其他類型之網路。本發明之一個具體例方案是可以用實物智慧卡(physical

(請先閱讀背面之注意事項再填寫本頁)

裝 · 訂 · 線

五、發明說明 (6)

smart card)；或是選擇用具有智慧卡相等功能與實效之電腦套裝軟體，安裝於例如個人電腦之計算裝置內運作。同樣的，一個商家(merchant)涉及一個銷售現場之收銀機式交易(point-of-sale)情況時，用商家的電腦主機(host computer)中的電腦套裝軟體與一個電子卡(EC)持卡人及一個服務提供者(service provider, SP)做交易通聯。若使用智慧卡時，就必需要與智慧卡之讀卡器一同使用，才能使智慧卡與商家的主機裝置能夠相連結上，主機裝置例如可以是一個網路線上待命(隨時可上網路)的商家終端電腦系統、可以是一台個人電腦、或是其他電子裝置其相容性足以支援做智慧卡電子交易處理。

在以公開金鑰暨電子憑證為機制之系統中，交易之參加人等，是用憑證中心CA或是用要約拘束之電子憑證伺服器(credentials binding server)所核發的電子憑證或用其他種類之電子證書達到相互間交換彼此的公開金鑰，電子憑證認證機構或是要約拘束之電子憑證伺服器，與所有各個參加交易者之間的所有通訊，都必是安全無慮的。本發明中亦使用複數個亂數(random numbers)與複數個電子簽章(digital signatures)以確保所有參加交易者間所傳送之資料的真實性暨有效性。

本發明亦使用非對稱性公開金鑰/私密金鑰之加密碼法，不過所運用之方式是有著些許不同，本發明之加密解密系統與方法並不是主張再去建立一套互信式關係，那一套例如早被周知的電子憑證持有者們與憑證中心們之間的

(請先閱讀背面之注意事項再填寫本頁)

訂
線

五、發明說明（ 7 ）

互信式關係。以大型會員為機制的金融機構是本發明的實作標的，例如大型信用卡公司及其會員們，或是主要大型銀行及其自動提款機會員們(ATM members)等等是本發明之潛在使用者。非金融機構亦可以經網路使用本加密解密系統與方法去執行電子商務或是非金融性電子交易。

一個服務提供者是會提供其所屬會員們某些類別的服務，正如一些金融機構就是提供其所屬會員們某一種類別的金融性服務；一個服務提供者本身也可以是非金融之屬性，但不論一個服務提供者是金融機構屬性還是非金融機構屬性，於本發明中其基本上皆是執行一個相同的交易過程；電子交易涉及金融機構，以及電子交易涉及非金融機構，兩者之間唯一不相同處是：交易資訊中分別含有互不相同的數據區域(data fields)。

經EC持卡人同意並與某一個服務提供者簽訂使用服務契約書後，該位服務提供者就會在EC持卡人的IC晶片記憶體內建立一個專屬數據槽(slot)，此專屬數據槽儲存包括該位服務提供者之帳戶應載資料、該位服務提供者的公開金鑰、持卡人用以控制通關之資料以及其他相關聯的數據。事先規劃每一張EC的IC晶片記憶體內所可容載之專屬數據槽數目(例如共計10個槽)，某一專屬數據槽就是某一服務提供者之代表。

藉著非對稱性公開金鑰之運用，金鑰散佈程序是很大地被簡化，於EC持卡人自己的電腦設備及場所、或是於同被持卡人與SP所互信之第三方例如於銀行專櫃、於郵

(請先閱讀背面之注意事項再填寫本頁)

裝
訂
線

五、發明說明(8)

局專櫃，都可以去執行安裝(load)服務提供者公開金鑰的工作。服務提供者公開金鑰是只限用於電子交易開始時的金鑰交換階段中EC持卡人等與服務提供者之間的通訊，完成金鑰交換階段之後，服務提供者會接著製發期間密鑰給EC持卡人等，期間密鑰是使用於保障服務提供者與EC持卡人等之間信息資料的安全交換，或是使用於持卡人等自己相互間之信息資料的安全交換。

本發明混合使用非對稱性公開金鑰密碼法暨對稱性私密金鑰密碼法(即，期間密鑰)，混合使用與單只使用對稱性私密金鑰密碼法之間的顯著不同處是：混合使用時其對稱性私密金鑰密碼法(意指期間密鑰)僅是於一個單一時段內有效用，並且期間密鑰不可以用於其它時段，一個時段(session)有一個預先設定好的有效時間期限，當超逾有效時間期限後或是當各項預設條件確經履行無誤後，期間密鑰就會失去使用效力。

商家與服務提供者之間信息資料的安全交換過程，基本上和服務提供者與持卡人之間的過程是一樣的，商家也是先向服務提供者交換得一把期間密鑰之後，以這把期間密鑰繼續與SP完成所有的交易通訊。持卡人與商家分別用其私密金鑰於傳送給服務提供者之每一份信息資料上做電子簽章，同樣的，服務提供者用其私密金鑰於回覆給商家及持卡人之每一份信息資料上做電子簽章。

當本發明之交易機制需要去與以電子憑證為交易機制的系統進行時，本系統的服務提供者於完成與商家及EC

(請先閱讀背面之注意事項再填寫本頁)

訂
線

五、發明說明（ 9 ）

持卡人之間的身分驗證並且也換完了期間密鑰之後，但當還需要再與其他外界系統做進一步的資訊交換或交易時，本系統之服務提供者正是以EC持卡人和商家的電子憑證代理人身分與電子憑證為交易機制的系統進行交易。換言之，服務提供者是用自其自己的電子憑證去代表商家們與EC持卡人等，和其他以電子憑證為交易機制的系統系統去完成交易。講個最遠的情況就是、本系統的服務提供者是履行電子憑證代理人的功能的角色，以及履行其做為會員們與以電子憑證為交易機制系統之間的一個閘道器(gateway)的角色。本發明這款種類的職階制是相當會受人想要的，因為，涉及各個不同系統之間的交易時，需要執行互信式關係驗證的機構數目將會因本發明這款職階制而大量減少。同時本發明也消除使用者需要一直持有有效之電子憑證才能參加某些線上交易的問題。

圖示簡單說明

第1圖為根據本發明之系統構成部份關係之一個具體例方塊圖；

第2圖為展示本發明之兩階段網路電子交易流程；

第3圖為電子卡之圖示；

第4圖為服務提供者們數據區之形態：每一個服務提供者之資料是分配於一個數據槽中，且數據槽是被某些存取控制方法所保護著；

第5圖為顯示本發明中使用電子簽章流程圖；

第6A至6Q圖展示例如於網際網路之開放型網路中，

(請先閱讀背面之注意事項再填寫本頁)

裝 · 訂 · 線

五、發明說明 (10)

本發明之電子交易中一種加密解密系統與方法的一個具體例流程圖；

第7至11圖為金鑰交換階段以及交易階段中，聯合換鑰要求信息、聯合換鑰回覆信息、聯合交易要求信息及聯合交易回覆信息之最終內容與格式表示圖；

第12圖展示一個服務提供者與交易參加者們間排成串行形態進行一個交易；

第13圖展示一個服務提供者與交易參加者們間於網路排成階層制組織形態進行一個交易。

詳細說明

本發明之較佳具體例是一種利用電子卡(EC)或電子卡之相等功能軟體，通聯至一個通訊網路後使用金鑰加密解密之系統與方法進行電子交易。

本發明之較佳具體例中，網路是一個公開型網路例如網際網路。本發明之其他具體例中，其他類別之公開型網路及/或封閉型網路均可以用以建立服務提供者與其會員們間的通聯，例如一個服務提供者可以提供其所私有的金融專屬網路與其會員們做通聯。

本發明可用任一種之網際網路通訊協定予以連結，可以用以連結之通訊協定例如包括：傳輸控制協定/跨網路協定之TCP/IP協定組、用戶郵包協定(UDP)、超文字傳輸協定HTTP等等之類。

通聯方式也可以使用網路傳送服務，例如使用類比電話服務的公共交換電話網路(PSTN)；或是使用數據通訊

(請先閱讀背面之注意事項再填寫本頁)

訂
線

五、發明說明 (11)

服務，例如使用寬頻T-1, E1, DS-3數據電路、整體服務數位網路(ISDN)、訂購者數據專線(DSL)，甚至使用無線服務等等之類。當使用上述中之一種服務，本發明被具體化實作時可獨立並自外於通訊協定(意指於一個電子介面層)。

通訊也可以經由區域網路(LAN)或是廣域網路(WAN)例如Ethernet區域網路，符記環網路(Token Ring)，光纖分散資料介面(FDDI)，非同步傳輸模式(ATM)等等之類，使用之通訊協定例如傳輸控制協定/跨網路協定之TCP/IP協定組，網際網路封包交換(IPX)，開放系統網接協定(OSI)等等之類。

其他通訊連結還可包括光纖式連結、無線頻率數據機連結、無線行動電話數據機連結、以及人造衛星網路連結等等。

當一個服務提供者與其所屬會員們間可以建立一個通訊路徑時，本發明就可以被利用之。以上列舉的是想意欲說明本發明可以實作於幾個不相同之通訊環境例子中。很清楚的，就拿通訊技術中之一般性技巧來說，本發明是完全不侷限於上述之幾個不相同之通訊環境例子中。

EC可以一片智慧卡之形式或是以一個套裝軟體之形式植於一部電腦中執行例如於一部個人電腦(PC)。當EC是以智慧卡之形式時，該卡可用於一個隨時可以上網路的電腦例如一部個人電腦，與另一個會員或是與其所選擇的服務提供者進行交易。交易進行時將需一個讀/寫介面裝

(請先閱讀背面之注意事項再填寫本頁)

裝
訂
線

五、發明說明 (12)

置做為卡與電腦間的通聯裝置，以及使用某種應用軟體例如一個網際網路流覽器做為持卡人與網路間之介面軟體。當 EC是以套裝軟體形式安裝於一個電腦系統時，那麼就不需要讀/寫介面裝置。本發明一個具體例是EC 當做電子錢包(electronic wallet)(或稱虛擬錢包)，一個功能與真正錢包相似之電子錢包。一個真正錢包能載有各種信用卡、轉帳卡(又稱扣帳卡)、自動提款卡、建保卡、會員卡及現金等等，一個EC具有上述各種金融工具性與非金融性工具的相等數據功能及能經網際網路執行安全交易。

所謂一個服務提供者之會員是指可以是一個商家或是一個EC持卡人。一個商家是指：一個經由服務提供者酬付交易之價金的會員。一個會員可以同時是商家及EC持卡人兩種身分。一個商家可與複數個EC持卡人進行一個交易，該個交易是終歸由服務提供者酬付交易之價金給商家。一個商家也可以同時是EC持卡人的身分例如去向一個貨品供應商購買貨品。

本發明之加密解密系統可含及一個服務提供者與複數個的服務提供者會員們間之通聯。通聯組合情況可以有：一個EC與一個SP；一個商家與一個SP；第一個EC與第二個EC與一個SP；以及第一個商家與第二個商家與一個SP等等交易組合。例如一個EC可以與一個服務提供者直接通聯做一個帳戶餘額資料查詢及帳戶清算查詢。一個商家可只代表其自己不代表其他EC可以與一個服務提供者通聯做其自己之帳頭餘額資料查詢及帳戶清算查詢。服務提

(請先閱讀背面之注意事項再填寫本頁)

訂
線

五、發明說明 (13)

供者與其會員們間之通聯可有各種情況的排列組合，其通聯組織之連結方式可以是串聯式和 / 或是職階制 (hierarchical)，服務提供者與其會員們間之通聯可以經路由器 (router) 轉送服務提供者與其會員們間之往返信息。

本發明之加密解密方法是一個兩個階段之金鑰交換 - 交易模式，第一個是金鑰交換階段，第二個是交易階段。於金鑰交換階段中，參加交易的會員們與服務提供者進行金鑰交換，參加交易的會員們將他們的公開金鑰傳給服務提供者之後，接著由服務提供者產製期間密鑰，服務提供者用會員們各個公開金鑰把期間密鑰做加密後傳給會員們。期間密鑰是被用來保護接著下來往返於EC持卡人等(會員們)與SP之間的信息；期間密鑰或是被用來保護EC持卡人(會員們)等自己互相之間所執行的信息傳送。於交易階段中，交易之進行可以是由SP去擔任者全程主導者或是由EC持卡人等自己去執行相互間之交易。

第1圖為根據本發明之系統構成部份關係之一個具體例方塊圖。圖中含有一個EC持卡人一個商家及一個服務提供者SP。

一個EC持卡人20可以經由網路50與商家執行一個交易，可使用交易源始電腦端上的EC讀/寫卡機82，或是使用具有EC相等功能之軟體92於交易源始電腦端上執行交易。

一個商家可以經由網路與被EC持卡人所挑選使用的服務提供者執行一個交易，商家可用隨時可以上網路的銷

(請先閱讀背面之注意事項再填寫本頁)

裝 · 訂 · 線

五、發明說明 (14)

售現場收銀終端機(point-of-sale terminal)40，或是用商家電腦端70中具有EC相等功能之軟體經由網路50例如網際網路，與被持卡人挑選使用的服務提供者60去執行一個交易。

只有使用識別條件及通關條件均是符合後，持卡人才可准經由網路50與其他交易參加者們去執行金融性或是非金融性的交易。第1圖中顯示經由網路有著三種不同之方案可以去執行一個交易。

(1)一個商家銷售現場交易POS(見第1圖左上端)，持卡人20於商家店鋪內將EC刷過/插入商家的EC讀/寫卡器30，EC讀/寫卡器是連結至一個網路線上待命(隨時可上網路)的商家終端電腦系統40，網路線上待命的商家終端電腦系統POS 40是一可抗拒竄改可被修改程式之裝置，輸入設備例如包括一個鍵盤、一個顯示器、一個中央位元處理器、以及一個電子卡讀/寫裝置30。通常它是一個小型電腦裝置，例如個人電腦裝有與開放型網路做連結的設備。商家終端電腦系統POS經由網路與SP做交易通聯。

(2)(見第1圖右端)一個持卡人把其EC 20插入連結於其個人電腦上的一個讀/寫裝置82可與本系統的交易參加者們執行一個交易，持卡人此端之電腦稱之為交易源始電腦端。交易源始電腦端經一個網路50與商家電腦端70做通聯，商家電腦端70中安裝有一個EC相等功能軟體72使商家可接收EC所製作發出的信息，該商家電腦70並可製作一個包含著EC資料與商家資料的聯合信息。然後商家把該聯合

(請先閱讀背面之注意事項再填寫本頁)

訂 線

五、發明說明 (15)

信息經由一個網路傳送至SP 60。

(3)(見第1圖下端)一個持卡人於顧客個人電腦端90執行EC相等功能軟體92可與本系統的交易參加者們執行一個交易，持卡人此端之電腦稱之為交易源始電腦端。持卡人經網路50與商家電腦端70做通聯後，再由商家經網路50與SP 60做通聯。

本發明之較佳具體例中，EC相等功能軟體是安裝於一部個人電腦中使用，本發明之另一具體實例是其他電子裝置可以植入EC相等功能軟體。

本發明之較佳具體實例中，用於使EC與商家做通聯之網路正是用於使商家與SP做通聯的相同一個網路。本發明之另一具體實例是，用於使EC與商家做通聯之網路可以不是用於使商家與SP做通聯的相同一個網路。本發明又另一具體實例是，用於使EC與商家做通聯之網路可以不是用於另一個EC與另一個商家做通聯的相同一個網路。本發明之一個具體例是可以由複數個網路所組成讓不同的參加交易者們進行通聯。

本發明之較佳具體例中，一個交易有兩個階段：一個金鑰交換階段及一個交易階段。第2圖是一個特別例，該特別例展示由SP所全程主導的一個兩個階段之金鑰交換-交易模式，SP所全程主導的整個交易過程中所有參加交易者們之間並無任何敏感性資料相互交流。

不論是由SP做從頭至尾完全主導第一及第二階段，或是SP只主導第一階段不主導第二階段，這兩種情況中

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明 (16)

金鑰交換階段的執行方法都是相同的。

但當第二個階段，交易階段只是持卡參加交易者們間做互相交易而不涉及SP時，EC持卡人們用第一階段中SP所製發的期間密鑰去執行相互間通聯及交易。

第2圖展示由SP全程主導交易階段的一個金融性交易。該交易含有三個單位：一個EC(是一個開始交易者)102，一個商家(merchant)，及一個服務提供者(SP) 106。源始交易端是一個消費持卡人並以一部電腦102做為表示，商家以一部電腦104做為表示，服務提供者SP以一部電腦106做為表示，服務提供者是經由EC挑選及商家所同意的。

第2圖展示一個金融性交易從一個EC至一個商家再至一個SP的過程。本發明之加密解密方法的流程是不侷限於EC及商家之間也不侷限於任何一個案流程順序。第2圖只是一個從EC至商家再至SP的交易流程個別案例。交易流程也是可以從商家至EC再至服務提供者SP。第2圖展示服務提供者的會員們(於此處指一個EC持卡人及一個商家)是如何格式化製作(format)、加附(attach)及傳送信息(message)至一個服務提供者SP的流程。

第2圖中共十個標記有1號至10號的箭頭是說明於兩階段交易中，信息(messages)是如何流程於三個交易單位(party)之間，步驟1至步驟4是屬於金鑰交換階段而步驟5至步驟10是屬於交易階段。第2圖中之流程例子展示商家是處於EC與SP之中間，在步驟1中，EC格式化製作其自

(請先閱讀背面之注意事項再填寫本頁)

訂 線

五、發明說明 (17)

己的金鑰交換要求信息(key exchange request message)傳送至商家。在步驟2中，商家製作(即格式化)其自己的金鑰交換要求信息後合併EC所製作金鑰交換要求信息後把EC-商家聯合金鑰交換要求信息(combined key exchange message)傳送至一個SP。在步驟3中，SP製作一個給EC的金鑰交換回覆息(key exchange response message)及一個給商家的金鑰交換回覆息，SP將兩個金鑰交換回覆信息做合併，形成一個SP金鑰交換聯合回覆EC-商家信息(combined key exchange response)後傳送至商家，在步驟4中，商家把SP回答商家的金鑰交換回覆信息以及SP回答EC的金鑰交換回覆信息從金鑰交換金鑰交換金鑰交換回覆EC-商家信息中分離出來，並把SP回答EC的金鑰交換回覆信息轉傳至EC，步驟4終結金鑰交換階段中的主要的活動。

從步驟5是開始第二階段--交易階段，在步驟5中，EC製作其自己的交易要求信息(transaction request message)傳送至商家。在步驟6中，商家製作其自己的交易要求信息後合併EC所製作的交易要求信息後把EC-商家聯合交易要求信息(combined transaction request message)傳送至SP。

在步驟7中，SP製作一個給EC的交易回覆信息(transaction response message for EC)及一個給商家的交易回覆信息，SP將兩個為交易回覆信息做合併，形成一個SP聯合交易回覆EC-商家信息(combined key exchange

(請先閱讀背面之注意事項再填寫本頁)

裝
訂
線

五、發明說明 (18)

response)後傳送至商家，在步驟8中，商家把SP回答商家的金鑰交換回覆信息以及SP回答EC的金鑰交換回覆信息從SP聯合交易回覆EC-商家信息中分離出來，並把SP回答EC的交易回覆信息轉傳至EC。在步驟9中，EC製作其自己的承認交易信息(confirmation message)傳送至商家。在步驟10中，商家製作其自己的承認交易信息後合併EC所製作的交易承認信息後把EC-商家聯合交易承認信息(combined confirmation message)傳送至SP。步驟10終結一個交易的第二階段。

第2圖雖展示了一個簡單的交易，但有一些交易可以涉及複數個信息，也就是一個階段之交易中需要有一個以上的信息才能去完成，即使是這種情況下，複數個信息之聯合要求及聯合回覆仍是遵循著相同一樣的流程規則去執行。例如在交易階段中，SP可能會要求EC及商家先將SP會員帳戶資料傳給SP，如果帳戶資料經SP確認為真實及有效後，SP才會植“帳戶資料已確認”的數據於回答EC及商家的回覆信息中，當商家及EC一收到SP所回覆的信息後，商家及EC把兩造交易價金及其他交易所需之資料植於下一個信息內後再一起傳給SP。SP接著決定是同意授權或是不同意授權該項交易之進行。第2圖中的各個步驟適用於帳戶信息及交易信息。

如果本交易系統需要與例如以電子憑證為交易機制108的外界系統(external system)做相互間資訊交換時，服務提供者SP刻正是以EC持卡人電子憑證代理人身分及商

(請先閱讀背面之注意事項再填寫本頁)

訂 線

五、發明說明 (19)

家的電子憑證代理人身分去與以電子憑證為交易機制的外界系統進行交易。本發明一個想要的結果就是：使得所有交易參加者可以防禦外界系統的入侵，因而可減少交易所需要的職階式互信關係。如果一個交易參加者同時擁有本系統會員身分以及外界系統會員身分，在後者之情形中，SP會用外界系統之機制與交易參加者做連繫。

第3圖是一個電子卡(EC)之較佳具體例圖示，在本發明之較佳具體例中，一個EC之內部是由軟體暨硬體零件所構建而成如第3圖所示。EC是國際標準組織編號ISO 7816，其並使用與ISO 7816相同的通訊規格與執行指令。

EC有一個控卡操作系統550用以管控EC卡內部的資源，卡上(on-card)密碼服務供應器650可以密碼軟體形式、或以密碼共同處理器(cryptographic co-processor)(未顯示於第3圖中)、或以其他密碼硬體設施、或以密碼軟體及密碼應體混合等方式予以實作。

EC的一個獨有特色是EC記憶體中的服務提供者資料區(service provider data area, SPDA)，SPDA存載著各個服務提供者之帳戶資料與金鑰資料。服務提供者資料區SPDA 700具有若干可容載之SP數據槽，在本發明之較佳具體例中，服務提供者數據區中包括一個事先制訂好的複數個數據槽(例如計有10個數據槽)，每一個數據槽是專屬於一個將來可能被使用的服務提供者。在本發明之另一具體例中，數據槽的數目可以是動態改變的，每一槽中之存檔包括有一個特定用途的服務提供者之帳戶號碼、公開金鑰、以

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明 (20)

及其他相關資料。

按不同的 EC 設計方式，SPDA 可以選擇性地允許每一個 SP 能植入一些軟體(例如使用一個爪哇 JAVA 術語中可獨立於作業平台的 applet 小程序)俾便管控 SP 自己的卡上數據，並藉由 applet 小程序去提供 SP 卡中數據與 SP 主控應用(host application)之間的介面。換言之，SPDA 不僅是可載有簡單之數據，EC 中的 SPDA 可讓每一位 SP 比存載一個完全獨立的應用軟體(例如 applet)俾提供其持卡會員們獨有的服務。這種方式的優點是 EC 其自己於此刻把其所能提供的服務做了個分離，每一個 SP 就可自己使用其所能提供服務的能力，如此，當另一個新的 SP 把卡上一個 SP 換下來時，EC 的作業平台就不需做任何更動，只需把新的 SP applet 應用軟體灌入卡後就會執行該軟體所設計之內容。

在 SPDA 中，每一個服務提供者的公開金鑰都會分配有其可儲存之空間位置，在很多交易中只有使用一對非對稱性公開金鑰，但也有一些線上交易是需要兩對以上的非對稱性公開金鑰；因此，當在信息接收之後與在信息被送出之前，如果 SP 均是用同一對非對稱性公開金鑰的話，那麼使用一對非對稱性公開金鑰就夠了，但如果 SP 用不同的非對稱性公開金鑰執行電子簽章，那麼 SPDA 中就需有兩對公開金鑰，一對用於信息接收後另一對用於信息送出前。

本發明之較佳具體例中是使用兩對非對稱性公開金鑰經網路與其它應用端執行溝通，因為使用兩對非對稱性公

(請先閱讀背面之注意事項再填寫本頁)

訂 線

五、發明說明 (21)

開金鑰是比只使用一對非對稱性公開金鑰較能提供更多一點的通訊安全保障。兩對中的第一對是用來對接收到的信息做解密，那就是送訊端用收訊端的公開金鑰將信息做加密，收訊端用配對的那一把私密金鑰將所收到信息做解密；第二對是送訊端用其私密金鑰將信息做電子簽章，收訊端用送訊端用配對那一把的公開金鑰將所收到信息做解密後執行確認電子簽章。

被每一個服務提供者使所用的複數個公開金鑰都會分配有其於SPDA中的儲存之空間，如果SP是用同一對非對稱性公開金鑰做送訊前電子簽章及收訊後解密的話，那麼用一對非對稱性公開金鑰就夠了，但如果SP用不同的非對稱性公開金鑰執行收訊後解密及送訊前電子簽章，那麼SPDA中就需儲有著兩對對公開金鑰。

在本發明之另一個具體例中，服務提供者就需二對以上的非對稱性公開金鑰去成就更高的交易安全性。

當EC持卡人已接受一個新的金融或非金融服務提供者所核發之服務時，經該核發機構、或是經持卡人與SP所互信之第三方將把所需要之數據資料安裝入一個空著的數據槽中；當要取消某一個服務提供者之帳戶時，該個服務提供者於SPDA數據槽中之資料就可被消除掉。數據槽中之一些資料例如帳戶號碼是可以被讀取但無法被寫改，一些資料例如私密金鑰是無法讀取及無法改寫。數據槽中之資料之存取條件600包括例如用個人身分識別通關密碼(PIN)或生物數據辨識法等，一個EC使用人想知道儲存卡

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明 (22)

中資料就必須提出卡片並完成正確之通關辨識。

傳統的個人身分識別通關密碼以及其他安全機制之識別方法例如生物數據辨識法均可以用以保護電子卡EC。生物數據辨識法是涉及持卡人複數個生物特徵的測量例如身體特徵及行為特徵，一個生物數據辨識法可以測量包括一個人的指紋、手的幾合形狀、手書寫字形、臉部表情樣子、講話聲音、身體動作、做電腦鍵盤輸入時的節奏感、眼睛部份的特徵(eye features)、呼吸氣之頻率、身體氣味、去氧核糖核酸DNA或是持卡人其他身體上的屬性特徵等。在所有通關條件均符合之後EC的功能才會被啟動。每一個服務提供者可自行植入其他想設定的通行條件於電子卡內。

第4圖展示較佳具體例中服務提供者們資料區SPDA之形態，每一個服務提供者的資料均是各自被分配登錄於卡中目錄區(table)的一個登錄間(entry)，登錄間是可以另外的通關條件加以保護。個人身分識別通關密碼PIN 712及其他數據區域(miscellaneous data filed)714使服務提供者能提供持卡人額外保護或是供給數據區域給其所要支援的裝置。

名稱區域702包括服務提供者們的名稱，一個線上交易(online transaction)將要開始時，首先持卡人由名稱區域中選擇其所要使用的服務提供者，金鑰種類區域704載有服務提供者是指定選擇使用那一種金鑰，例如使用對稱性公開金鑰或是非對稱性私秘金鑰(secret key)等，金鑰值

(請先閱讀背面之注意事項再填寫本頁)

訂
線

五、發明說明 (23)

區域706(key value)及帳戶資料區域708含及屬於各個服務提供者獨一無二的資料。卡種類區域710用以指明某個服務提供者所支援之載具種類(例如是信佣卡或是提款卡)。

本發明之較佳具體例中，卡上操作系統(on-card operating system, COS)提供持卡人一些基本服務，下表列出一些COS能執行的通常性功能：

- (1)傳統OS功能--例如記憶管理及工作管理等等。
- (2)持卡人資料與外界之讀/寫通訊作業以及通訊協定處置。
- (3)安裝及更新持卡人之卡上資料。
- (4)持卡人變更卡上之個人識別通關密碼PIN。
- (5)服務提供者資料區管理--例如安裝及更新卡上服務提供者個別之資料以及SPDA存取管控等等。

COS亦於一個交易的不同階段之中提供支援，例如COS可以處理一個交易要開始時之選擇SP，及交易完成後把交易記錄至一個紀錄檔案中。本發明之另一個具體例中，可以實行下列兩種COS設計門徑中之一種，或是以下列兩種設計門徑之混合實作之：

- (1)大部份的智能均可以植入COS並藉以支援大部份的EC功能，其結果是每一個卡上服務提供者區域賴以COS去完成EC與商家及SP之間的交易，在這一種設計門徑中，COS能提供所有卡上SP一個與外面世界間的一個統一介面，使一但一個SP被EC挑選中並經商家同意之後能夠有效地完成交易。

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明 (24)

(2)另一種是，COS是一個共享利用的共通服務，是由每一個卡上SP共享利用之，每一個SPDA可以包含applets應用軟體，applets具有去完成EC與商家及SP之間交易所需要具備之智能，在這一種設計門徑中，當執行一個交易時SP有較多的機會去實行其自己的獨有特色。

第5圖展示在本發明之較佳具體例中是如何去使用電子簽章流程：一個送訊端首先把一個信息M之資料部份*900(data portion of a message M)輸入一個單向雜湊演算法(one way hash algorithm)中，H(*) 902，其經由單向雜湊演算法生成之輸出又稱之為信息M之數據部份*之信息摘要MD(message digest, MD)(有譯稱簽體、文件彙記)903，然後用送訊端EC的私密金鑰把信息摘要MD做加密，E(*) 904，加密也就是做電子簽章之意思，其結果稱為信息M之數據部份*之電子簽章(DS)。然後把DS信息與M之資料部份*900做合併(加附)形成一個完整的送訊端之源始信息906後就可以隨時經由網路傳送至一個接收端。

公開金鑰密碼器可以是若干個公開金鑰密碼器中之一個；RSA非對稱性公開式密碼器的名稱由來是取自三位發展人(Ronald Rivest, Adi Shamir, and Len Adelman)姓名的首個英文字母予以合成，RSA密碼器是只是一個非對稱性公開金鑰私密金鑰一個例子，RSA密碼器可被用於本發明一個具體例中。

當事先預定的收訊端從網路50收到源始信息後，收訊端首先把加附在一再起的信息M之數據部份*900與電子簽

(請先閱讀背面之注意事項再填寫本頁)

訂 線

五、發明說明 (25)

章DS 912予以分離開來，收訊端把信息M之數據部份*900輸入與送訊端有著相同功能的一個單向雜湊演算法910，該單向雜湊演算法把信息M之數據部份*生成一個信息M之數據部份*之準信息摘要MD[^] 911。收訊端接著用送訊端的公開金鑰把包含於源始信息中的電子簽章DS做解密D(*) 908，得以復原源始信息摘要，在此處以MD 909做標記，MD 909與新生成(演算得)的MD[^] 911做比較後，若兩者之值是不相等時，則表示源始(originating)信息已有訛誤且必須予以廢棄。

第5至11圖中所使用符號及縮寫說明做列表如下：

Acknowledgement DataEC = EC承認交易數據；是信息之一部份從EC傳給SP，該數據告知SP前一個信息已被成功地接到到並依約定處理完畢。

Acknowledgement DataM = 商家承認交易數據；是信息之一部份從商家傳給SP該數據並告知SP前一個信息已被成功地接收到並依約定處理完畢。

AI_{EC} = EC持卡人帳戶資料(EC cardholder account information)

AI_M = 商家帳戶資料(merchant account information)

CRYPTO = 密文(cryptogram)

D = 執行解密功能(Decryption)

D_{SP-Private-Key} = 使用SP私密金鑰做解密

DS = 電子簽章(功能)(Digital Signature)

DS_{EC-Private-Key} = EC使用其私密金鑰把一個信息做簽章所

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明 (26)

形成之電子簽章

$DS_{M-Private-Key}$ = 商家使用其私密金鑰把一個信息做簽章所
形成之電子簽章

$DS_{SP-Private-Key}$ = SP用其私密金鑰把一個信息做簽章所形成
之電子簽章

E = 執行加密功能(Encryption)

$E(Data)$ = 使用一把加密金鑰把數據執行(做)加密

E_{SP-PK} , $E_{SP-Public-Key}$ = 使用SP公開金鑰把數據執行(做)加密

$E_{Skey-EC}$, $D_{Skey-EC}$ = 使用SP所產製並指定(傳送)給EC之EC
期間密鑰執行加密或是解密

E_{Skey-M} , D_{Skey-M} = 使用SP所產製並指定(傳送)給商家之商
家期間密鑰執行加密或是解密

EC = 電子卡(Electronic Card)或是與電子卡具有相等功能
之軟體

$H(M)$ = 應用一個單向雜湊演算法(a one way hashing
algorithm)於M後生成信息M之信息摘要(MD)

KE = 金鑰交換(Key Exchange), 換鑰

M = 商家(Merchant)

MD = 信息摘要(又稱簽體)(Message Digest)

$MD^{\wedge}$ = 把收訊端用適才收到之信息輸入一個單向雜湊演
算法所輸出得到之準信息摘要(又稱準簽體)

MD_{EC} = EC信息摘要; 從EC傳至SP信息之EC信息摘要

MD_M = M(商家)信息摘要; 從商家傳至SP信息之商家信息
摘要

(請先閱讀背面之注意事項再填寫本頁)

訂 線

五、發明說明 (27)

MD_{SP-M} = SP-M 信息摘要；從 SP 傳至商家信息之 SP 信息摘要

MD_{SP-EC} = SP-EC 信息摘要；商家居間做轉傳之一個從 SP 傳至 EC 信息之 SP 信息摘要

PLAIN TEXT = 明文；勿需加密即可傳送之交易資料；明文因信息不同及不同之參加交易者會有不同

PLAIN TEXT_{EC} = EC 明文；EC 即將傳送出的信息中之一部份勿需加密交易資料。明文之數據區域乃非安全上敏感，故傳送之間不執行加密。使用明文符號於不同信息中時其內容會有不同

PLAIN TEXT_{TM} = 商家明文；商家即將傳送出的信息中之一部份勿需加密交易資料。明文之數據區域乃非安全上敏感，故傳送之間不執行加密；使用明文符號於不同信息中時其內容會有不同

PLAIN TEXT_{SP-EC} = SP-EC 明文；SP 即將傳送給 EC 時的信息中之一部份勿需加密交易資料。明文之數據區域乃非安全上敏感，故傳送之間不執行加密；使用明文符號於不同信息中時其內容會有不同

PLAIN TEXT_{SP-M} = SP-M 明文；SP 即將傳送給商家時的信息中之一部份勿需加密交易資料。明文之數據區域乃非安全上敏感，故傳送之間不執行加密；使用明文符號於不同信息中時其內容會有不同

S_{TD} = 敏感性交易數據(sensitive transaction data)，傳送之間需要執行加密

(請先閱讀背面之注意事項再填寫本頁)

裝 · 訂 · 線

五、發明說明 (28)

$STD_{EC} = (EC)$ 電子卡敏感性交易數據；EC即將傳送出的信息中之敏感性交易數據；使用敏感性交易數據於不同信息中時其內容會有不同

$STD_M =$ 商家敏感性交易數據；商家即將傳送出的信息中之敏感性交易數據；使用敏感性交易數據符號於不同信息中時其內容會有不同

PK= 公開金鑰(Public Key)

EC-PK, $PK_{EC} = (EC)$ 電子卡公開金鑰

M-PK, $PK_M =$ 商家公開金鑰

SP-PK, $PK_{SP} =$ 被挑選使用之服務提供者公開金鑰

$Response\ Data_{SP-EC} =$ SP-EC交易回覆數據；一個交易的交易階段中SP回覆給EC信息中之一部份交易數據；可包括同意交易之數據或是不同意交易之數據，及或其他相關數據

$Response\ Data_{SP-M} =$ SP-M交易回覆數據；一個交易的交易階段中SP回覆給商家信息中之一部份交易數據；可包括同意(製發交易授權碼)交易的數據或是不同意交易的數據，及或其他相關數據

RN = 亂數(random number)

$RN_{EC} =$ EC亂數；EC所產製之亂數EC用以傳至SP

$RN_{SP-EC} =$ SP-EC亂數；SP所產製之亂數SP用以傳至EC

$RN_M =$ 商家亂數；商家所產製之亂數商家用以傳至SP

$RN_{SP-M} =$ SP-M亂數；SP所產製之亂數用以傳至商家

SP = 金融性或非金融性服務提供者(Service Provider)

(請先閱讀背面之注意事項再填寫本頁)

訂 線

五、發明說明 (29)

TA = 交易(幣別)金額(Transaction Amount)

Transaction Identification Number_{SP-EC}, TID_{SP-EC} (Transaction ID_{SP-EC}) = SP-EC交易辨識碼；一個交易之金鑰交換階段中被SP所產製並指定(傳送)給 EC的數據區；EC會用之該數據區之值與SP於同一個交易中做通聯。

Transaction Identification Number_{SP-M}, TID_{SP-M} (Transaction ID_{SP-M}) = SP-M交易辨識碼；一個交易之金鑰交換階段中被SP所產製並指定(傳送)給商家的數據區；商家會用之該數據區之值與SP於同一個交易中做通聯辨識。

* = 一個加密功能中或是一個解密功能中執行數據間的合併、加附(attach)、聯合(combine)或連結(concatenate)

第6A至6Q圖展示例如於網際網路之開放型網路中，本發明之電子交易中一種加密解密系統與方法的一個具體例流程圖。為了簡化含於第6A至6Q圖中的敘述及符號，第6圖之流程圖是假設每一位參加交易者均是使用一對公開金鑰；本發明之另一個具體例中是使用兩對公開金鑰，該例中之兩對公開金鑰均需要予以做金鑰交換。

本發明之較佳具體例中一個交易是包含有兩個階段：一個金鑰交換階段接續一個交易階段。

第一階段：金鑰交換階段(PHASE I: KEY EXCHANGE PHASE)。亦稱握手協商階段(HANDSHAKE PHASE)

EC持卡人把EC插入一個讀/寫卡器之插槽或是啟動EC相等功能軟體，接著EC持卡人輸入正確的各项通關存取條件，例如生物數據辨識法(biometrics data)之後才能

(請先閱讀背面之注意事項再填寫本頁)

裝 · 訂 · 線

五、發明說明 (30)

取得用卡權。EC所輸入的安全資料條件與卡上原存通關存取條件資料114做比較112以驗證用卡人是否已被授權使用該EC卡。如果輸入之安全資料與卡上原存安全資料不符時，則用卡要求被拒116，不然的話EC卡就會被開啟使用118。當EC卡被開啟後用卡人可以要求列示卡上所有可供選用的SP名單並對EC發出執行一個挑選SP的指令後挑選一個SP 120。當一個SP被挑選中後，EC開始進行與SP做金鑰交換(KE)。被挑選中的SP公開金鑰是以符號SP-PK及 PK_{SP} 符號為代表， PK_{SP} 是從EC的SPDA中取得，用以把信息做加密後傳給SP。

KE之主要目的是安全地將持卡人之EC公開金鑰 PK_{EC} 126及EC亂數 RN_{EC} 124傳給SP。之後，SP會產製並指定一個期間密鑰及一個SP-EC交易辨識碼 TID_{SP-EC} 並回覆(傳送)給EC，EC收到後據以為此後與SP做通聯與交易的確認用途。首先，欲格式化EC的KE信息時，首先EC產製一個意欲傳至SP的EC亂數 RN_{EC} 124，EC把EC亂數 RN_{EC} 與EC公開金鑰 PK_{EC} 126及與交易相關或是SP所規定的敏感性數據 STD_{EC} 128三項連結一起後，用從SPDA 120中所檢索挑選而取得的SP公開金鑰 PK_{SP} 做加密122，所計算得之EC密文 $E_{SP-PK}(RN_{EC} * PK_{EC} * STD_{EC})$ ，再與信息之明文部份EC明文PLAIN TEXT $_{EC}$ 132做合併130--意指如果EC有明文要傳給SP時，至此形成一個EC(合併而成之)換鑰要求信息之數據部份：PLAIN TEXT $_{EC} * E_{SP-PK}(RN_{EC} * PK_{EC} * STD_{EC})$ 。每當要組成一個EC要求信息時，EC公開金鑰 PK_{EC} 126也可

(請先閱讀背面之注意事項再填寫本頁)

訂
線

五、發明說明 (31)

以選擇植於EC明文PLAIN TEXT_{EC}中，就不必被加密。

只有敏感性數據才要加密，非敏感性數據是含於明文中，整個交易中僅有SP可以讀取各個參加交易者所傳送的敏感性數據，在一個有複數個參加者的交易中，僅有SP對所有交易參加者的敏感性數據具有完全存取權(full access)。

所計算得的EC密文再輸入一個單向雜湊演算法134後得一雜湊值(hash message)(又稱簽體或稱文件彙記)，該雜湊值就是EC信息摘要MD_{EC}，EC使用私密金鑰138把EC信息摘要MD_{EC}做簽章136形成一個EC電子簽章DS_{EC-Private-Key}，EC把EC把電子簽章DS_{EC-Private-Key}及EC換鑰要求信息之數據部份合併一起140，就是將信息之明文部份EC明文PLAIN TEXT_{EC}，EC密文CRYPTO_{EC-Private-Key}及EC電子簽章DS_{EC-Private-Key}合併一起，至此一個EC換鑰要求信息於焉組成：[PLAIN TEXT_{EC}*E_{SP-PK}(RN_{EC}*PK_{EC}*STD_{EC})]*DS_{EC-Private-Key}。EC換鑰要求信息經由一個網路傳送至商家158。明文含及所有各種非敏感性之交易數據區域，由於不具敏感性因此可以一個透明可辨之形式做傳送不需加密。這些交易數據區域在不同信息中時其內容會有所不同，且這些交易數據區域是由各個交易參加者自己去下定義。

商家意欲與SP做通聯時，也就是商家想組成商家與SP間之這一段KE信息時，商家則也是去經歷組成EC與商家間之KE信息的那一段本質上相同的步驟。持卡人及商家絕不單獨地與SP做通聯而是以一個EC信息及一個商家信

五、發明說明 (32)

息所合併而成之聯合信息與SP做通聯，其結果就是持卡人與商家之間根本不必互相交換他們的任何機密性金融資料，商家準備好其自己用以做交易的裝備142並從存駐於商家裝備SPDA中檢索出與EC持卡人已挑選為該個交易所使用的同一個SP 144，被挑選中的SP公開金鑰 是以符號SP-PK及 PK_{SP} 符號為代表，是從商家的SPDA中取得，用以把信息做加密後傳給SP。

商家欲格式化自己的KE信息時，首先商家產製一個意欲傳至SP的商家亂數 RN_M 148，商家把商家亂數 RN_M 與商家公開金鑰 PK_M 150及與交易相關或是SP所規定的敏感性數據STDEC 152三項連結一起後，用由商家設備SPDA 144中所檢索而得的SP公開金鑰 PK_{SP} 做加密146，所計算得的商家密文 $E_{SP-PK}(RN_M*PK_M*STD_M)$ ，再與信息之明文部份商家明文PLAIN TEXT $_M$ 156做合併154--意指如果商家有明文要傳給SP時，至此一個商家(合併而成之)要求信息於焉組成： $PLAIN TEXT_M*E_{SP-PK}(RN_M*PK_M*STD_M)$ ，每當要去組成一個商家要求信息時，商家公開金鑰PKEC 150也可以植於商家明文PLAIN TEXT $_M$ 中，就不必被加密。商家換鑰要求信息 $[PLAIN TEXT_M*E_{SP-PK}(RN_M*PK_M*STD_M)]$ 進一步與EC換鑰要求信息 $\{[PLAIN TEXT_{EC}*E_{SP-PK}(RN_{EC}*PK_{EC}*STD_{EC})]*DS_{EC-Private-Key}\}$ 做合併158形成一個EC-商家聯合換鑰要求信息之數據部份(data portion of the KE request message)， $[PLAIN TEXT_{EC}*E_{SP-PK}(RN_{EC}*PK_{EC}*STD_{EC})]*DS_{EC-Private-Key}\}$ $*[PLAIN TEXT_M*E_{SP-PK}(RN_M*PK_M$

(請先閱讀背面之注意事項再填寫本頁)

訂
線

經濟部智慧財產局員工消費合作社印製

五、發明說明 (33)

*STD_M)]。商家接著再把EC-商家聯合換鑰要求信息之數據部份輸入一個單向雜湊演算法160後生成一個雜湊值(又稱簽體)，該值就是商家信息摘要MD_M，商家使用商家私密金鑰164對商家信息摘要MD_M做簽章162形成一個商家電子簽章DS_{M-Private-Key}，商家把商家電子簽章DS_{M-Private-Key}及EC-商家聯合換鑰要求信息之數據部份做合併166，也就是把明文PLAIN TEXT_M，密文CRYPTO_{M-Private-Key}及商家電子簽章DS_{M-Private-Key}合併一起形成EC-商家最終聯合換鑰要求信息後經由一個網路傳送至SP168<<{[PLAIN TEXT_{EC} *E_{SP-PK}(RN_{EC}*PK_{EC}*STD_{EC})]*DS_{EC-Private-Key}}*[PLAIN TEXT_M*E_{SP-PK}(RN_M*PK_M*STD_M)]>>*DS_{M-Private-Key}。第7圖展示金鑰交換階段中，從商家傳至SP之EC-商家聯合換鑰要求信息之最終內容與格式表示圖。

本發明之較佳具體例中，由於EC已對其公開金鑰已經做了加密之故，商家就不必拿EC換鑰要求信息去執行一次信息摘要MD_{EC}檢查。

本發明之另一個具體例中，當EC不對其公開金鑰做加密的話，那麼商家可以選擇性地在尚未把EC-商家最終聯合換鑰要求信息傳送至SP之前對EC所傳至商家之EC換鑰要求信息先執行信息摘要檢查。上述之任一具體例中，不論是EC對其公開金鑰已做加密與否，為了提高安全度及避免商家自己處理時恐致生任何可能的錯誤，SP仍是可以檢查EC換鑰要求信息的信息摘要。當商家收到SP傳來的一部份要給他自己及其餘部份SP要商家轉傳給EC之

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明 (34)

最終聯合換鑰回覆信息時，商家則就不必替EC檢查信息摘要，因為要商家轉傳給EC的這一部份換鑰回覆信息是SP最終聯合換鑰回覆信息之一部份且這些數據均是由SP這同一個源始產製者(originator)所製作傳送出的，故商家只需對從SP傳來的整一個最終聯合換鑰回覆信息做信息摘要檢查即可。

當SP收到商家傳來的EC-商家最終聯合換鑰要求信息時，SP首先把EC-商家最終聯合換鑰要求信息之數據部份與商家電子簽章 $DS_{M-Private-Key}$ 做分離168 並把EC-商家最終聯合換鑰要求信息之數據部份輸入一個單向雜湊演算法後生成一個準雜湊值(又稱準簽體)，該準雜湊值就是商家準信息摘要 MD^M ，SP接著把商家明文 $PLAIN\ TEXT_M$ 、商家密文 $CRYPTO_M$ 、商家電子簽章 $DS_{M-Private-Key}$ 與EC-商家最終聯合換鑰要求信息之數據部份中的EC換鑰要求信息 $PLAIN\ TEXT_{EC} * CRYPTO_{EC} * DS_{EC-Private-Key}$ 做分離。SP用其自己的私密金鑰把商家密文做解密170，並復原(recovered)，尤其是商家亂數 RN_M 148 及商家公開金鑰 PK_M 150，SP然後用復原的商家公開金鑰 PK_M 把商家電子簽章 $DS_{M-Private-Key}$ 做解密並復原EC-商家最終聯合換鑰要求信息之商家信息摘要 MD_M 。SP把新演算而得的商家準信息摘要 MD^M 168與把EC-商家最終聯合換鑰要求信息之 $DS_{M-Private-Key}$ 做解密而復原的商家信息摘要 MD_M 170做比較172，如果 MD^M 與 MD_M 發現彼此是矛盾，則EC-商家最終聯合換鑰要求信息已遭訛誤因此必須予以廢棄174；

(請先閱讀背面之注意事項再填寫本頁)

訂 線

五、發明說明 (35)

如果 $MD^{\wedge}_M$ 與 MD_M 兩值是相等，則 SP 續把 $DS_{EC-Private-Key}$ 與 EC 換鑰要求信息之數據部份做分離 176(1)，並把 EC 換鑰要求信息之數據部份輸入一個單向雜湊演算法後生成一個 EC 準信息摘要 MD_{EC} ，SP 接著把 EC 換鑰要求信息的數據部份中之 EC 明文 $PLAIN\ TEXT_{EC}$ 、EC 密文--意指如果有 EC 密文時、及 EC 電子簽章 $DS_{EC-Private\ Key}$ 做分離 176(2)。然後 SP 用其自己的私密金鑰把 EC 密文做解密 176(3)，並復原，尤其是 EC 亂數 RN_{EC} 124 及 EC 公開金鑰 PK_{EC} 126，SP 然後用 EC 公開金鑰 PK_{EC} 把 EC 電子簽章 $DS_{EC-Private-Key}$ 做解密並復原 EC 換鑰要求信息之 EC 信息摘要 MD_{EC} 。在步驟 178 中，SP 把新演算得的 EC 準信息摘要 $MD^{\wedge}_{EC}$ 176 與原先的最終聯合換鑰要求信息中之 $DS_{EC-Private-Key}$ 做解密而復原的 EC 信息摘要 MD_{EC} 做比較，如果 $MD^{\wedge}_{EC}$ 與 MD_{EC} 發現彼此是矛盾，則表示最終聯合換鑰要求信息已遭訛誤因此必須予以廢棄 180；如果 $MD^{\wedge}_{EC}$ 與 MD_{EC} 兩值是相等，SP 就開始準備回傳一個 EC-商家最終聯合換鑰回覆信息，該信息是 SP 先傳給商家後再由商家做出分離後再由商家轉傳 EC 之部份給 EC。

SP 欲格式化一個換鑰回覆信息給 EC 時，首先 SP 產製一個意欲傳給 EC 之 SP-EC 亂數 $RNSP-EC$ 184 及產製一個意欲傳給 EC 的 SP-EC 期間密鑰(session key) 186 ($SkeySP-EC$)，並將此兩項及 EC 產製之 EC 亂數 $RNEC$ 188 (見步驟 124)，以及 SP 給 EC 的 SP-EC 敏感性交易數據 190 $STDSP-EC$ 等四項用 SP 於步驟 176(3) 中解密而得的 EC 之公開金鑰一

(請先閱讀背面之注意事項再填寫本頁)

裝 · 訂 · 線

五、發明說明 (36)

起做合併 182。該合併所計算出來的 SP-EC 密文 $E_{EC-PK}(RN_{SP-EC} * RN_{EC} * Skey_{SP-EC} * STD_{EC})$ 再與 SP 指定傳送給 EC 之 SP-EC 交易辨識碼 194 及 SP 給 EC 之 SP-EC 明文 PLAIN TEXT_{SP-EC} 196--意指如果 SP 有明文要傳送給 EC 的話，等等一起做合併 192，形成一個 SP 之換鑰回覆 EC 信息之數據部份。SP 把換鑰回覆 EC 信息之數據部份輸入一個單向雜湊演算法後生成一個 SP-EC 信息摘要 MD_{SP-EC} 198。SP 用自己的私密金鑰對 SP-EC 信息摘要 MD_{SP-EC} 做簽章 200 形成一個 SP 電子簽章 $DS_{SP-Private-Key}$ ，接著 SP 把 SP 電子簽章 $DS_{SP-Private-Key}$ 及 SP 要回傳給 EC 的 SP 之換鑰回覆 EC 信息之數據部份合併一起 204，至此 SP 要回傳給 EC 的一個 SP 換鑰回覆 EC 信息已構建完成： $[TID_{SP-EC} * PLAIN\ TEXT_{SP-EC} * E_{EC-PK}(RN_{SP-EC} * RN_{EC} * Skey_{SP-EC} * STD_{EC})] * DS_{SP-Private-Key}$ 。

SP 欲格式化一個 SP 換鑰回覆信息給商家時，首先 SP 產製一個意欲傳給商家之 SP-M 亂數 RN_{SP-M} 208 及產製一個 SP 意欲傳給商家的 SP-M 期間密鑰 (session key) 210 $Skey_{SP-M}$ ，並將此兩項及商家產製之商家亂數 212 (見步驟 148) RNM 、以及 SP 給商家的 SP-M 敏感性交易數據 214 STD_{SP-M} 等四項一起用 SP 於步驟 170 中解密而得的商家公開金鑰一起做合併 206 形成 SP 要回覆給商家之 SP-EC 密文 $E_{M-PK}(RN_{SP-M} * RN_M * Skey_{SP-M} * STD_{SP-M})$ ，該合併所計算出來之 SP-EC 密文再與 SP 所指定傳送給商家之 SP-M 交易辨識碼 218 及 SP 給商家之 SP-M 明文 PLAIN TEXT_{SP-M} 220--意指如果 SP 有明文要傳送給商家的話，等等一起做合併 220。

(請先閱讀背面之注意事項再填寫本頁)

訂 線

五、發明說明 (37)

至此SP要回傳給商家的一個SP換鑰回覆商家信息已構建完成： $TID_{SP-M} * PLAIN \quad TEXT_{SP-M} * E_{M-PK}(RN_{SP-M} * RN_M * Skey_{SP-M} * STD_{SP-M})$ 。

SP接著把SP要回傳給商家的換鑰回覆商家信息 $TID_{SP-M} * PLAIN \quad TEXT_{SP-M} * E_{M-PK}(RN_{SP-M} * RN_M * Skey_{SP-M} * STD_{SP-M})$ 與SP要回傳給EC的換鑰回覆EC信息： $[TID_{SP-EC} * PLAIN \quad TEXT_{SP-EC} * E_{EC-PK}(RN_{SP-EC} * RN_{EC} * Skey_{SP-EC} * STD_{EC})] * DS_{SP-Private-Key}$ 一起做合併222形成SP回答EC與商家的一個SP最終換鑰聯合回覆EC-商家信息之數據部份： $[TID_{SP-EC} * PLAIN \quad TEXT_{SP-EC} * E_{EC-PK}(RN_{SP-EC} * RN_{EC} * Skey_{SP-EC} * STD_{EC})] * DS_{SP-Private-Key} * [TID_{SP-M} * PLAIN \quad TEXT_{SP-M} * E_{M-PK}(RN_{SP-M} * RN_M * Skey_{SP-M} * STD_{SP-M})]$ 。

SP把要回答商家與EC之最終換鑰聯合回覆EC-商家信息之數據部份輸入一個單向雜湊演算法後生成一個SP-M信息摘要 MD_{SP-M} 224。SP用自己的私密金鑰228對該SP-M信息摘要 MD_{SP-M} 做簽章226形成一個SP電子簽章 $DS_{SP-Private-Key}$ ，接著SP把形成的SP電子簽章 $DS_{SP-Private-Key}$ 226及SP要回傳給商家及EC的最終換鑰聯合回覆EC-商家信息之數據部份合併一起230，至此，一個SP回答商家與EC之最終聯合換鑰回覆EC-商家信息於焉形成並經由一個網路傳送至商家： $<<\{[TID_{SP-EC} * PLAIN \quad TEXT_{SP-EC} * (E_{EC-PK} * RN_{SP-EC} * RN_{EC} * Skey_{SP-EC} * STD_{EC})] * DS_{SP-Private-Key}\} * [TID_{SP-M} * PLAIN \quad TEXT_{SP-M} * E_{M-PK}(RN_{SP-M} * RN_M * Skey_{SP-M} * STD_{SP-M})]>> * DS_{SP-Private-Key} = [(TID_{SP-EC} * PLAIN \quad TEXT_{SP-Private-Key} * CRYPTO_{SP-EC})$

(請先閱讀背面之注意事項再填寫本頁)

裝 · 訂 · 線

經濟部智慧財產局員工消費合作社印製

五、發明說明 (38)

$*DS_{SP-Private-Key}*(TID_{SP-M}*PLAIN\ TEXT_{SP-M}*CRYPTO_{SP-M})*$
 $DS_{SP-Private-Key}$ ，第8圖展示金鑰交換階段中，從SP傳至商家後再由商家轉傳至EC的SP之最終聯合換鑰回覆EC-商家信息之內容與格式表示圖。

當商家接收到SP傳來之最終聯合換鑰回覆EC-商家信息232時，首先商家將SP簽過章的SP電子簽章 $DS_{SP-Private-Key}$ 做出分離232(1)，商家接著把最終聯合換鑰回覆EC-商家信息之數據部份輸入一個單向雜湊演算法232(2)後生成一個SP-M準信息摘要 MD^{SP-M} ，接下來商家就把SP回答商家與EC之最終聯合換鑰回覆EC-商家信息之數據部做分離232(3): TID_{SP-M} 、 $PLAIN\ TEXT_{SP-M}$ 、 $CRYPTO_{SP-M}$ 、 $[(TID_{SP-EC}*PLAIN\ TEXT_{SP-EC}*CRYPTO_{SP-EC})]*DS_{SP-Private-Key}$ ，接著商家用SP公開金鑰（於步驟144所檢選）把從最終聯合換鑰回覆EC-商家信息中所分離出來的SP電子簽章 $DS_{SP-Private-Key}$ 做解密232(4)復原SP-M信息摘要 MD_{SP-M} 。在步驟234中，SP把新演算得的SP-M準信息摘要 MD^{SP-M} 232(2)與從最終聯合換鑰回覆EC-商家信息之 $DS_{SP-Private-Key}$ 做解密而復原的 MD_{SP-M} 232(4)做比較，如果 MD^{SP-M} 與 MD_{SP-M} 發現彼此是矛盾，則最終聯合換鑰回覆EC-商家信息已遭訛誤因此必須予以廢棄236；如果 MD^{SP-M} 與 MD_{SP-M} 兩值是相等時，商家則去辨識於最終聯合換鑰回覆信息中那些是SP意欲回覆給他的部份，用商家自己的私密金鑰把SP密文 $CRYPTO_{SP-M}$ 做解密後238，商家應可復原商家亂數 RN_M （見步驟148），該商家亂數 RN_M 是商家曾經植入於其換鑰要求

（請先閱讀背面之注意事項再填寫本頁）

訂線

五、發明說明 (39)

信息中之後所傳給SP的。在步驟240中，商家把復原的商家亂數 RN_M 與(源始)商家亂數 RN_M 148做比較240，如果兩值不相等，則最終聯合換鑰回覆EC-商家信息已遭到訛誤因此必須予以廢棄242；正因為僅有SP自己用SP的私密金鑰才有可能把亂數 RN_M 復原，此就已保證了回覆內容的信息傳送端正是SP無誤。之後商家才會把SP要傳給EC的SP之換鑰回覆EC信息 $[(TID_{SP-EC} * PLAIN \text{ TEXT}_{SP-EC} * CRYPTO_{SP-EC})] * DS_{SP-Private-Key}$ 轉傳給EC。商家於此開始為第二階段--交易階段做準備。

當EC接收到商家轉傳來之SP換鑰回覆EC信息260時，首先EC將SP簽過章的SP電子簽章 $DS_{SP-Private-Key}$ 做分離260(1)，EC接著把SP換鑰回覆EC信息之數據部份輸入一個單向雜湊演算法後生成一個SP-EC準信息摘要 MD^{SP-M} ，接下來EC就把SP回答EC的SP換鑰回覆EC信息之數據部份做分離260(2)： TID_{SP-EC} 、 $PLAIN \text{ TEXT}_{SP-EC}$ 、 $CRYPTO_{SP-EC}$ 、 $DS_{SP-Private-Key}$ ，接著EC用SP公開金鑰(於步驟120所檢選)把從SP之換鑰回覆EC信息中所分離出來的SP電子簽章 $DS_{SP-Private-Key}$ 做解密260(3)復原SP-EC信息摘要 MD_{SP-EC} 。在步驟262中，SP把新演算得的SP-EC準信息摘要 MD^{SP-EC} 260(1)與從SP換鑰回覆EC信息之 $DS_{SP-Private-Key}$ 做解密而復原的 MD_{SP-EC} 260(3)做比較262，如果 MD^{SP-EC} 與 MD_{SP-EC} 發現彼此是矛盾，則SP之換鑰回覆EC信息已遭訛誤因此必須予以廢棄264；如果 MD^{SP-EC} 與 MD_{SP-EC} 兩值是相等時，EC辨識回覆信息中那些是SP意欲回覆給他的部份，EC用

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明 (40)

自己的私密金鑰把SP-EC密文CRYPTO_{SP-EC}做解密後266，EC應可復原EC亂數RN_{EC}(見步驟124)，該EC亂數RN_{EC}是EC曾經植入於換鑰要求信息中之後傳給SP的。在步驟268中，EC把復原的EC亂數RN_{EC}與(原始)EC亂數RN_{EC} 124做比較，如果兩值不相等，則SP換鑰回覆EC信息已遭到訛誤因此必須予以廢棄270；正因僅有SP用正確的SP私密金鑰才能復原亂數RN_{EC}，此就已保證了回覆內容的信息傳送端正是SP無誤。EC於此開始為第二階段--交易階段做準備。

電子交易之前將是會有一個事先就制定好的暫停期(timeout period)植於EC處及商家處。在一個交易中，某一個回覆信息若是沒有於一個暫停期內被送訊端收到的話，EC與商家就會認定該個交易是失敗(aborted)，EC與商家會執行重試要不然就會該開始執行回收程序(recovery process)。

當成功地完成各個KE信息交換後，至此算一算，SP持有EC公開金鑰及商家公開金鑰；EC持有一個SP給的SP-EC亂數、EC持有一個SP給的SP-EC交易識別碼、以及EC持有SP給的一把期間密鑰；商家持有一個SP給的SP-M亂數、商家持有一個SP-M交易識別碼、以及商家持有SP給的一把期間密鑰。只有EC把接收到並復原的SP-EC亂數再傳回SP且被SP驗證為有效之時，以及商家把接收到並復原的SP-M亂數再傳回SP且被SP驗證為有效之時，金鑰交換階段才算是完成。有兩種方式可以去完成：上述亂數

(請先閱讀背面之注意事項再填寫本頁)

訂 線

五、發明說明 (41)

可被分別植於EC與商家回覆SP的一個聯合承認交易信息中(a confirmation message)，或者是例如於第二階，即、於交易階段中把亂數植於一個交易信息中並當成EC經商家至SP所回應SP的某一個EC-商家聯合回應信息的一部份數據。後者方法是比較簡易些並於下列詳做說明。亂數只被使用一回，那就是用以確保SP與商家之間以及SP與EC之間金鑰交換的正確性，一但奠立了期間密鑰及交易識別碼之後，亂數就停止使用。

第二階段--交易階段(PHASE II: TRANSACTION PHASE)

在交易階段中，商家及EC各自傳送他們自己的資料例如帳戶號碼、及其他與交易有關之數據例如交易價金、申請授權交易(碼)、或是其他處理數據給SP。再一次地，EC及商家是各自與SP進行電子商務交談，是經由EC-商家聯合信息與SP做商談，即，商家收到EC的信息之後就負責把EC信息及商家自己的信息合併一起成為一個聯合信息後傳給SP。

首先EC把交易信息做格式化處理，EC把SP給EC的亂數 RN_{SP-EC} 274、被EC挑選用於該次交易的EC持卡人於SP之帳戶資料 AI_{EC} 276、該次交易EC與商家均已同意之交易價金(金額) TA 280、及與交易相關或是SP所規定的EC敏感性數據278 STD_{EC} 四項連結一起後，用SP所產製並指定傳送給EC的EC期間密鑰 $Skey_{EC}$ 做加密272。 $Skey_{EC}$ 是一種密秘金鑰密碼法(對稱性私密金鑰/私密金鑰)例如DES密碼器(Data Encryption Standard)，其所使用的

(請先閱讀背面之注意事項再填寫本頁)

裝
訂
線

五、發明說明 (42)

密碼演算法與對非稱性公開金鑰/私密金鑰所使用的密碼演算法是不一樣。

所計算得之EC密文 $CRYPTO_{EC}$ ，即 $Skey_{EC}(RN_{SP-EC} * STD_{EC} * AI_{EC} * TA)$ ，再與SP給EC的SP-EC交易辨識碼284，信息之明文部份 $PLAIN\ TEXT_{EC}$ 286--意指如果EC有明文要傳送給SP時，等等一起做合併282形成一個EC交易要求信息之數據部份： $TID_{SP-EC} * PLAIN\ TEXT_{EC} * CRYPTO_{EC}$ 。EC把EC交易要求信息之數據部份282輸入一個單向雜湊演算法後生成一個EC信息摘要 MD_{EC} 288。EC用自己的私密金鑰292對該EC信息摘要 MD_{EC} 做簽章290形成一個EC電子簽章 $DS_{EC-Private-Key}$ ，接著EC把形成的電子簽章 $DS_{EC-Private-Key}$ 290及EC要傳給SP的EC交易要求信息之數據部份282合併一起294，至此一個EC交易要求信息於焉組成： $[TID_{SP-EC} * PLAIN\ TEXT_{EC} * Skey_{EC} (RN_{SP-EC} * STD_{EC} * AI_{EC} * TA)] * DSEC-Private-Key$ ，EC交易要求信息經由一個網路傳送至商家。

本質上商家是使用與EC格式化EC之交易要求信息一樣的步驟去格式化商家交易要求信息。首先商家把交易信息做格式化處理，商家把SP給商家的亂數--SP亂數 RN_{SP-M} 246(見步驟208及步驟238)、被EC挑選經商家同意用於該次交易的商家於SP之帳戶帳戶資料 AI_M 248、該次交易EC與商家均已同意之交易價金(金額) TA 252、及與交易相關或是SP所規定的商家敏感性數據250 STD_M 四項連結一起後，用SP所產製並指定傳送給商家之期間密鑰 $Skey_M$ (見步

(請先閱讀背面之注意事項再填寫本頁)

訂
線

五、發明說明 (43)

驟210及步驟238)做加密244。Skey_M是一種密秘金鑰密碼法(對稱性私密金鑰/私密金鑰)例如DES密碼器(Data Encryption Standard)，其所使用的密碼演算法與對非稱性公開金鑰/私密金鑰所使用的密碼演算法是不一樣。於此Skey_M是被用來對數據加密後形成密文CRYPTO_M。

所計算得之商家密文CRYPTO_M，即Skey_M(RN_{SP-M}*STD_M*AIM*TA)，再與SP給商家的SP-M交易辨識碼256，信息之明文部份PLAIN TEXT_M 258--意指如果商家有明文要傳給SP時，等等一起做合併254形成一個商家交易要求信息之數據部份：TID_{SP-M}*PLAIN TEXT_M*CRYPTO_M。

商家把商家交易要求信息之數據部份254與EC交易要求信息294做合併296形成一個EC-商家最終聯合交易要求之數據部份：[TID_{SP-EC}*PLAIN TEXT_{EC}*Skey_{EC}(RN_{SP-EC}*STD_{EC}*AI_{EC}*TA)]*DS_{EC-Private-Key} [TID_{SP-M}*PLAIN TEXT_M*Skey_M(RN_{SP-M}*STD_M*AIM*TA)]。與先前之做法一樣，EC-商家最終聯合交易要求之數據部份輸入一個單向雜湊演算法後生成一個商家信息摘要MD_M 298。商家用自己的私密金鑰302對該商家信息摘要MD_M做簽章300形成一個商家電子簽章DS_{M-Private-Key}，接著商家把形成的商家電子簽章DS_{M-Private-Key} 300及EC-商家要傳給SP的EC-商家最終聯合交易要求信息之數據部份296合併一起304，至此一個EC-商家最終聯合交易要求信息於焉組成：{[TID_{SP-EC}*PLAIN TEXT_{EC}*Skey_{EC}(RN_{SP-EC}*STD_{EC}*AI_{EC}*TA)]*DS_{EC-Private-Key} [TID_{SP-M}*PLAIN TEXT_M*Skey_M(RN_{SP-M}*STD_M*AIM*

(請先閱讀背面之注意事項再填寫本頁)

裝
訂
線

五、發明說明 (44)

TA)]]*DS_{M-Private-Key}，EC-商家最終聯合交易要求信息經由一個網路傳送至商家。第9圖展示交易階段中，從商家傳至SP之EC-商家最終聯合要求交易信息之內容與格式表示圖。

五、發明說明 (45)

以廢棄314；如果 MD^M 與 MD_M 兩值是相等，則 SP接著用換鑰階段中SP所產製並指定傳送給商家的商家期間密鑰 $Skey_M$ （見步驟210）把商家要求交易信息中之商家密文 $CRYPTO_M$ 做解密312後復原密文中的數據，SP把與SP於換鑰階段所產製並傳至商家之SP亂數（見步驟208） RN_{SP-M} 與於步驟316復原的SP亂數 RN_{SP-M} 做比較316，如果兩個SP亂數 RN_{SP-M} 之值不相等，那麼商家就是沒有通過商家與SP之間的相互驗證檢測，該個交易信息予以廢棄320。

如果兩個SP亂數 RN_{SP-M} 之值是相等，此時，SP會驗證EC的帳戶資料 AI_{EC} 以及交易資料例如交易價金TA，如果帳戶資料 AI_{EC} 以及交易資料經SP驗出不再是有效或不完全符合SP的交易條件時SP會把交易信息廢棄320。若商家傳至SP的交易價金TA與EC傳至SP的交易價金TA，經SP驗出兩值並不相等時，SP會把交易信息廢棄。如果EC的帳戶資料 AI_{EC} 及交易資料均正確，SP繼續檢查信息中有關EC的部份。

至於商家交易要求信息，首先SP把 $DS_{EC-Private-Key}$ 從EC交易要求信息中分離出來322(1)，並把EC交易要求信息之數據部份($TID_{SP-EC} * PLAIN\ TEXT_{EC} * CRYPTO_{EC}$)輸入322(2)一個單向雜湊演算法後生成一個EC交易要求信息數據部份之EC準信息摘要 MD^M_{EC} ，SP用EC公開金鑰把 $DS_{EC-Private-Key}$ 做解密復原EC信息摘要 MD_{EC} 324，在步驟326中，SP把新演算得的EC準信息摘要 MD^M_{EC} 322(2)與復原324所得的EC信息摘要 MD_{EC} 做比較，如果 MD^M_{EC} 與 MD_{EC}

（請先閱讀背面之注意事項再填寫本頁）

裝

訂

線

五、發明說明 (46)

發現彼此是矛盾，則表示EC-商家最終聯合交易要求信息已遭訛誤因此必須予以廢棄328；如果 $MD_{EC}^{\wedge}$ 與 MD_{EC} 兩值是相等，則 SP 接著用換鑰階段中 SP 所產製並指定傳送給商家的 EC 期間密鑰 $Skey_{EC}$ (見步驟186) 把商家要求交易信息中之商家密文 $CRYPTO_{EC}$ 做解密330後復原密文中的數據，SP 把與 SP 於換鑰階段所產製並傳至商家之 SP-EC 亂數 (見步驟184) RN_{SP-EC} 與於步驟330復原的 SP-EC 亂數 RN_{SP-EC} 做比較332，如果兩個 SP-EC 亂數 RN_{SP-EC} 之值不相等，那麼商家就是沒有通過商家與 SP 之間的相互驗證檢測，該個交易信息予以廢棄334。如果兩個 SP-EC 亂數 RN_{SP-EC} 之值是相等。此時，SP 會驗證商家的帳戶資料 AI_M 以及交易資料例如交易價金 TA，如果帳戶資料 AI_M 以及交易資料經 SP 驗出不再是有效時或不全符合 SP 的條件時 SP 會把交易信息廢棄334。若商家傳至 SP 的交易價金 TA 與 EC 傳至 SP 的交易價金 TA，SP 驗出兩值並不相等時，SP 會把交易信息廢棄334。

只有整個的 EC-商家最終於聯合交易要求信息完的整性與驗證性被 SP 奠立之後，SP 才能進行處理 EC-商家最終聯合交易要求信息中的數據及去回傳一個 SP 最終聯合交易回覆 EC-商家信息。商家及 EC 回傳給 SP 的兩個 SP 亂數： RN_{SP-M} 及 RN_{SP-EC} ，經 SP 比對為正確時就表示 SP 與商家之間，以及 SP 與 EC 之間已完成相互間的驗證，從此處以後的步驟中就不再需要去執行任何亂數交換。SP 亦可選擇使用該等亂數當成交易辨識碼 TID，從此處以後的步驟

(請先閱讀背面之注意事項再填寫本頁)

訂
線

五、發明說明 (47)

中商家把 RN_{SP-M} 當成交易辨識碼 TID_{SP-M} 植於商家給 SP 的信息中；以及從此處以後的步驟中 EC 把 RN_{SP-EC} 當成交易辨識碼 TID_{SP-EC} 植於 EC 給 SP 的信息中。

與前面所述之方法雷同，最終聯合交易回覆信息含及 SP 要回覆給 EC 及商家的資料。欲格式化一個 SP 交易回覆信息給 EC 時，首先 SP 產製其要回應 EC 的 SP-EC 交易回應數據 $Response\ Data_{SP-EC}$ 338 並用 SP 產製並指定傳送給 EC 的 EC 期間密鑰 $Skey_{EC}$ (見步驟 186) 做加密 336 形成 SP-EC 密文 $CRYPTO_{SP-EC}$ ，意指當 SP 有敏感性數據要給 EC 時才要被加密，非敏感性數據則被植於明文中。SP 接著把 SP-EC 密文 $CRYPTO_{SP-EC}$ 即， $E_{Skey-EC}(Response\ Data_{SP-EC})$ 、SP 產製並指定傳送給 EC 的 SP-EC 交易辨識別碼 342 TID_{SP-EC} (見步驟 194)、SP 要給 EC 的明文 $PLIAN\ TEXT_{SP-EC}$ 344-- 意指如果 SP 有明文要傳給 EC 的話，等三項一起做合併 340 形成 SP 之交易回覆 EC 信息之數據部份： $TID_{SP-EC} * PLIAN\ TEXT_{SP-EC} * E_{Skey-EC}(Response\ Data_{SP-EC})$ ，SP 之交易回覆 EC 信息之數據部份輸入一個單向雜湊演算法 346 生成一個 SP-EC 信息摘要 MD_{SP-EC} ，接著用 SP 私密金鑰 350 把 SP-EC 信息摘要 MD_{SP-EC} 做簽章 348 形成一個 SP 電子簽章 $DS_{SP-Private-Key}$ ，SP 把 SP 電子簽章 $DS_{SP-Private-Key}$ 與 SP 之交易回覆 EC 信息之數據部份做合併 352，一個 SP 交易回覆 EC 信息於焉形成： $[TID_{SP-EC} * PLIAN\ TEXT_{SP-EC} * E_{Skey-EC}(Response\ Data_{SP-EC})] * DS_{SP-Private-Key}$ 。

欲格式化一個 SP 交易回商家覆信息給商家時，首先 SP

(請先閱讀背面之注意事項再填寫本頁)

裝 · 訂 · 線

五、發明說明 (48)

產製其要回應商家的SP-M交易回應數據Response Data_{SP-M} 356 並用SP產製並指定傳送給商家的商家期間密鑰Skey_M (見步驟210)做加密354形成SP密文CRYPTO_{SP-M} --意指SP有敏感性數據要傳給商家時才要被加密，非敏感性數據則被植於明文中。SP接著把SP密文CRYPTO_{SP-M}即，E_{Skey-M}(Response Data_{SP-M})、SP產製並指定傳送給商家的SP-M交易辨識碼360 TID_{SP-M} (見步驟218)、SP要給商家的明文PLIAN TEXT_{SP-M} 362-意指如果SP有明文的話，等三項一起做合併 358形成一個SP交易回覆商家信息之數據部份： $TID_{SP-M} * PLIAN\ TEXT_{SP-M} * E_{Skey-M}(Response\ Data_{SP-M})$ 。

SP之交易回覆商家信息之數據部份358與一個SP交易回覆EC信息352做合併364形成SP之最終聯合交易回覆EC-商家信息之數據部份： $[TID_{SP-EC} * PLIAN\ TEXT_{SP-EC} * E_{Skey-EC}(Response\ Data_{SP-EC})] * DS_{SP-Private-Key} * [TID_{SP-M} * PLIAN\ TEXT_{SP-M} * E_{Skey-M}(Response\ Data_{SP-M})]$ 。SP把SP之最終聯合回覆交易EC-商家信息之數據部份輸入366一個單向雜湊演算法後生成一個SP-M信息摘要MD_{SP-M}，SP用SP私密金鑰370把SP-M信息摘要MD_{SP-M}做簽章 368形成一個SP電子簽章DS_{SP-Private-Key}，接著SP把SP電子簽章DS_{SP-Private-Key} 368與最終聯合交易回覆EC-商家信息之數據部份364做合併 372，一個最終聯合交易回覆EC-商家信息於焉形成： $\{[TID_{SP-EC} * PLIAN\ TEXT_{SP-EC} * E_{Skey-EC}(Response\ Data_{SP-EC})] * DS_{SP-Private-Key}\} * [TID_{SP-M} * PLIAN\ TEXT_{SP-M} * E_{Skey-M}(Response\ Data_{SP-M})] >> * DS_{SP-Private-Key}$ 。第10圖展示交易

(請先閱讀背面之注意事項再填寫本頁)

訂
線

經濟部智慧財產局員工消費合作社印製

五、發明說明 (49)

階段中，從SP傳至商家之SP最終聯合交易回覆EC-商家信息之內容與格式表示圖。

當商家收到SP傳來的SP最終聯合回覆交易EC-商家信息，首先商家檢查374(1)該信息中的SP-M交易辨識碼 TID_{SP-M} （見步驟218及步驟232）是否有效，如果SP-M交易辨識碼 TID_{SP-M} 是無效的，商家就把SP聯合交易回覆EC-商家信息予以廢棄376，如果SP-M交易辨識碼 TID_{SP-M} 是有效的，商家把SP用其私密金鑰做簽章所形成的SP電子簽章 $DSSP-Private-Key$ 與SP最終聯合回覆交易EC-商家信息之數據部份做分離374(2)，商家把最終聯合交易回覆EC-商家信息之數據部份 $[TID_{SP-EC} * PLIAN \text{ TEXT}_{SP-EC} * E_{Skey-EC}(\text{Response Data}_{SP-EC})] * DS_{SP-Private-Key} * [TID_{SP-M} * PLIAN \text{ TEXT}_{SP-M} * E_{Skey-M}(\text{Response Data}_{SP-M})]$ 輸入374(3)一個單向雜湊演算法後生成一個SP-M準信息摘要 $MD^{\wedge}_{SP-M}$ ，接著商家把SP交易回覆商家信息之數據部份做分離374(4)： TID_{SP-M} 、 $PLIAN \text{ TEXT}_{SP-M}$ 、 $E_{Skey-M}(\text{Response Data}_{SP-M})$ 。商家開始準備把 $[TID_{SP-EC} * PLIAN \text{ TEXT}_{SP-EC} * E_{Skey-EC}(\text{Response Data}_{SP-EC})] * DS_{SP-Private-Key}$ 轉傳給EC。

商家用SP於金鑰交換階段所產製並指定傳送給商家的商家期間密鑰 $Skey_M$ （見步驟210及步驟238）把SP-M密文 $CRYPTO_{SP-M}$ 做解密378復原含於其中之數據，商家用SP公開金鑰（見步驟144）把SP電子簽章 $DSSP-Private-Key$ 做解密378(3)復原SP-M信息摘要 MD_{SP-M} ，商家把新演算得的SP-M準信息摘要 $MD^{\wedge}_{SP-M}$ 與復原的 MD_{SP-M} 做兩值比較380

（請先閱讀背面之注意事項再填寫本頁）

裝 · 訂 · 線

五、發明說明 (50)

，如果 MD^{SP-M} 與 MD_{SP-M} 不相等，則表示 SP 最終聯合交易回覆 EC-商家信息已遭訛誤因此必須予以廢棄 382；如果 MD^{SP-M} 與 MD_{SP-M} 兩值是相等，則商家開始處理所收到之信息數據，與前面曾述及過程一樣，商家把 SP 之交易回覆 EC 信息轉傳給 EC 380。

當 EC 收到商家轉傳來的一個 SP 之交易回覆 EC 信息，EC 首先檢查該信息中的 SP-EC 交易辨識碼 TID_{SP-EC} (見步驟 194 及步驟 260) 是否有效，如果 SP-EC 交易辨識碼 TID_{SP-EC} 是無效的，EC 就把 SP 之交易回覆 EC 信息予以廢棄 396，如果 SP-EC 交易辨識碼 TID_{SP-EC} 是有效的，EC 把以 SP 私密金鑰做簽章所形成的 SP 電子簽章 $DS_{SP-Private-Key}$ 與 SP 之交易回覆 EC 信息之數據部份做分離 394(2)，EC 把 SP 之交易回覆 EC 信息之數據部份 $[TID_{SP-EC} * PLIAN TEXT_{SP-EC} * E_{Skey-EC} (Response Data_{SP-EC})]$ 輸入 394(3) 一個單向雜湊演算法後生成一個 SP-EC 準信息摘要 MD^{SP-EC} ，接著 EC 把 SP 之交易回覆 EC 信息之數據部份做分離 394(4)： TID_{SP-EC} 、 $PLIAN TEXT_{SP-EC}$ 、 $E_{Skey-EC} (Response Data_{SP-EC})$ 。

EC 用 SP 於金鑰交換階段所產製並指定傳送給 EC 的期間密鑰 $Skey_{EC}$ (見步驟 186 及步驟 266) 把密文 $CRYPTO_{SP-EC}$ 做解密 378(1) 復原含於其中之數據，EC 用 SP 公開金鑰 (見步驟 120) 把 $DS_{SP-Private-Key}$ 做解密 378 復原 MD_{SP-M} ，商家把新演算得的 SP-EC 準信息摘要 MD^{SP-EC} 與復原的 MD_{SP-EC} 做兩值比較 400，如果 MD^{SP-EC} 與 MD_{SP-EC} 不相等，則表示 SP 之交易回覆 EC 信息已遭訛誤因此必須予以廢棄 402；如

(請先閱讀背面之注意事項再填寫本頁)

訂
線

五、發明說明 (51)

果 $MD_{SP-EC}^{\wedge}$ 與 MD_{SP-EC} 兩值是相等，則 EC 開始處理所收到之信息數據。

在整個交易流程之最末時刻，EC 與商家可以這麼去做--如果這也是於 SP 的要求條件之一的話，那就是，EC 與商家各傳送一個商家承認交易信息(an acknowledgement message)及一個 EC 承認交易信息給 SP，EC-商家用以承認 SP 最終聯合回覆 EC-商家交易信息內容是正確且處理完畢。

承認交易數據 Acknowledgement Data 可被分別植於 EC 與商家回應 SP 的一個最終聯合 EC-商家承認交易信息中(a confirmation message)，或者是例如於第二階段，即、於交易階段終結之前把承認交易數據植於一個交易信息中並當成 EC 經商家至 SP 所回應 SP 之某一個 EC-商家聯合回應信息的一部份數據。或是 EC 與商家把承認交易數據製作成單一獨立的信息傳送給 SP。

EC 欲格式 EC 承認交易信息時，EC 把承認數據的敏感性部份 406--意指如果 EC 有敏感性承認數據要傳給 SP 的話，EC 用 SP 所產製並指定傳送給 EC 的 EC 期間密鑰(見步驟 186 及步驟 266) $Skey_{EC}$ 做加密 404 形成 EC 密文 $CRYPTO_{EC}$ 。EC 把前面 SP 傳給 EC 的 SP-EC 交易辨識碼 TID_{SP-EC} 410 (見步驟 194 及步驟 260)、EC 明文-意指如果 EC 有明文 $PLAIN TEXT_{EC}$ 要傳給 SP 的話 412 等三項做合併 408 形成一個 EC 承認交易信息之數據部份： $TID_{SP-EC} * PLAIN TEXT_{EC} * Skey_{EC}$ (Acknowledgement Data_{EC})。

(請先閱讀背面之注意事項再填寫本頁)

裝
訂
線

五、發明說明 (52)

接著EC把EC承認交易信息之數據部份輸入414一個單向雜湊演算法生成一個EC信息摘要 MD_{EC} ，EC用其自己的私密金鑰418做簽章416形成一個EC電子簽章 $DS_{EC-Private-Key}$ ，EC把EC電子簽章 $DS_{EC-Private-Key}$ 與EC承認交易信息之數據部份408做合併420形成一個EC承認交易信息： $[TID_{SP-EC} * PLAIN \text{ TEXT}_{EC} * Skey_{EC} (Acknowledgement \text{ Data}_{EC})] * DS_{EC-Private-Key}$ ，EC把EC承認交易信息經網路傳至商家。

商家以和EC同樣的步驟去形成商家承認交易信息，欲格式化商家承認交易信息時，商家把承認數據的敏感性部份Acknowledgement Data_M 386--意指如果商家有敏感性承認數據要傳給SP的話，用SP所產製並指定傳送給商家的商家期間密鑰(見步驟210及步驟238) $Skey_M$ 做加密 384形成商家密文CRYPTO_M。商家把前面SP傳給商家的SP-M交易辨識碼 TID_{SP-M} 410 (見步驟218及步驟232)、商家明文-意指如果商家有明文PLAIN TEXT_M的話392等三項做合併388形成一個商家承認交易信息之數據部份： $TID_{SP-M} * PLAIN \text{ TEXT}_M * Skey_M (Acknowledgement \text{ Data}_M)$ 。

接下來商家把商家承認交易信息之數據部份與EC傳至商家的EC承認交易信息做合併422形成一個EC-商家聯合承認交易信息之數據部份： $\{[TID_{SP-EC} * PLAIN \text{ TEXT}_{EC} * Skey_{EC} (Acknowledgement \text{ Data}_{EC})] * DS_{EC-Private-Key}\} * [TID_{SP-M} * PLAIN \text{ TEXT}_M * Skey_M (Acknowledgement \text{ Data}_M)]$ 。

商家把EC-商家聯合承認交易信息之數據部份輸入

(請先閱讀背面之注意事項再填寫本頁)

訂線

五、發明說明 (53)

424一個單向雜湊演算法生成一個商家信息摘要 MD_M ，商家用其自己的私密金鑰428做簽章426形成一個商家電子簽章 $DS_{M-Private-Key}$ ，商家把商家電子簽章 $DS_{M-Private-Key}$ 與EC-商家聯合承認交易信息之數據部份422做合併430形成一個EC-商家最終聯合承認交易信息： $\ll\{[TID_{SP-EC}*PLAIN\ TEXT_{EC}*Skey_{EC}\ (Acknowledgement\ Data_{EC})]*DS_{EC-Private-Key}\}*[TID_{SP-M}*PLAIN\ TEXT_M*Skey_M\ (Acknowledgement\ Data_M)]\gg*DS_{M-Private-Key}$ 。商家把EC-商家最終聯合承認交易信息經由網路傳至SP。第11圖是展示交易階段中，從商家傳至SP之EC-商家最終聯合承認交易信息之內容與格式表示圖。

TID_{SP-M} 是SP產製並指定傳送給商家的SP-M交易辨識碼(見步驟218)， TID_{SP-EC} 是SP產製並指定傳送給EC的SP-EC交易辨識碼(見步驟194)。當SP收到從商家傳來之EC-商家最終聯合交易確認信息時商家首先就去檢查432(1) TID_{SP-M} 及 TID_{SP-EC} 這兩個交易辨識碼是否均是有效，如果 TID_{SP-M} 及 TID_{SP-EC} 兩者中之一個是無效時，SP把EC-商家最終聯合交易確認信息予以廢棄434；如果 TID_{SP-M} 及 TID_{SP-EC} 兩者均是有效時，SP接著把 $DS_{M-Private-Key}$ 與EC-商家最終聯合承認交易信息之數據部份做分離432(2)，SP把EC-商家最終聯合承認交易信息之數據部份輸入一個單向雜湊演算法生成一個商家準信息摘要MDM，SP把EC-商家最終聯合承認交易信息之數據部份做分離432(4)： TID_{SP-M} 、 $PLAIN\ TEXT_M$ 、 $Skey_M\ (Acknowledgement\ Data_M)$

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明 (54)

、 $TID_{SP-EC} * PLAIN \quad TEXT_{EC} * Skey_{EC} \quad (Acknowledgement \quad Data_{EC})] * DS_{EC-Private-Key} \circ$

SP 用商家的公開金鑰PKM (見步驟150及步驟170)把商家電子簽章 $DS_{M-Private-Key}$ 做解密436復原商家信息摘要 MD_M ，SP把新演算得的商家準信息摘要 $MD^M_{432(3)}$ 與復原的商家信息摘要 MD_M 436做兩值比較438，如果 MD^M 與 MD_M 不相等，則表示EC-商家承認交易信息已遭訛誤因此必須予以廢棄440；如果 MD^M 與 MD_M 兩值是相等，商家用SP於金鑰交換階段所產製並指定傳送給商家的期間密鑰 $Skey_M$ (見步驟210及步驟238)把商家密文 $CRYPTO_M$ 做解密442取得含於其中之商家承認交易數據Acknowledgement Data_M；

接著SP把EC承認交易信息之數據部份與EC電子簽章 $DS_{EC-Private-Key}$ 做分離444(1)，SP把EC承認交易信息之數據部份輸入一個單向雜湊演算法生成一個EC準信息摘要 MD^EC ，SP把EC承認交易信息之數據部份做分離444(2)： TID_{SP-EC} 、 $PLAIN \quad TEXT_{EC}$ 、 $Skey_{EC} \quad (Acknowledgement \quad Data_{EC})$ ，SP用EC的公開金鑰 PK_{EC} (見步驟126及步驟176)把EC電子簽章 $DS_{EC-Private-Key}$ 做解密446復原EC信息摘要 MD_{EC} ，SP把新演算得的EC準信息摘要 $MD^EC_{444(2)}$ 與復原的 MD_{EC} 446做兩值比較448，如果 MD^EC 與 MD_{EC} 不相等，則表示EC承認交易信息已遭訛誤因此必須予以廢棄450；如果 MD^EC 與 MD_{EC} 兩值是相等，商家用SP於金鑰交換階段所產製並指定傳送給EC的期間密鑰 $Skey_{EC}$ (見步驟186

(請先閱讀背面之注意事項再填寫本頁)

訂

線

五、發明說明 (55)

及步驟266)把EC密文CRYPTO_{EC}做解密452取得含於其中之EC承認交易數據Acknowledgement Data_{EC}。

至此，電子交易中之交易階段的所有過程已全部完成454。

在整個交易的期間，本發明之一個較佳具體例中，EC是與網際網路流覽器軟體所支援的介面軟體共同執行，該介面軟體例如是指微軟公司的探險家流覽器中(Microsoft Explorer)或是指在美國線上公司的網景領航員流覽器中(Netscape Navigator)。在一個典型例子的時段中，持卡人點選其所使用的流覽器至商家的固定資源定位器URL(uniform Resource Locator)後進入商家網站中進行向商家訂購貨品或是訂購服務，在EC決定要執行線上即時付款給商家之刻，流覽器會援用(invok)該EC介面軟體；該EC介面軟體可以是流覽器構造之一部份，或可以是流覽器的插座式(plug-in)之軟體元件或補充式(add-on)之軟體元件。EC持卡人可以用其流覽器點選連接任何一位SP會員的URL。

前面第6A至6Q圖中所描述的兩階段交易只是一個應用本發明之兩階段金鑰交換-交易模式時的一個特例。在第6A至6Q圖中所描述的兩階段交易中，交易參加者是一共有三位：EC、商家、及SP。同樣地本發明之兩階段金鑰交換-交易模式可以應用於含及參加交易者之數目是二位以上至多位；在一個含及三位以上參加交易者之情況中，是僅有一位是擔任SP的角色，且所有參加交易者們皆

(請先閱讀背面之注意事項再填寫本頁)

裝
訂
線

五、發明說明 (56)

是用相同一把被挑選中的SP之公開金鑰去執行開使時的金鑰交換，所有參加交易者們接著使用SP所產製並指定分配的期間密鑰及交易辨識碼去執行交易。

本發明之兩階段金鑰交換-交易模式可以應用於組織形態的方案，(1)參加交易者們可以與可能的複數個路由器與SP做成一個串聯排列；或者，(2)參加交易者們可以與可能的複數個路由器及與SP做成一個職階式組織排列；這些增多出來的職階式組織排列之中有可能含及複數個路由器，經由一個網路路徑把信息傳遞至鄰接層次(next level)。在職階式組織中的一個層次裏，是可以由任何數目的交易參加者及/或由任何數目的路由器所組成。鄰接層次是指串聯排列或職階式組織排列中，與下一個交易參加者或下一個路由器所鄰接的層次。在一個職階式組織排列的方案中，鄰接層次含及所有可能數目的鄰接交易參加者及所有可能數目的鄰接路由器。在職階式組織排列方案中，是由SP建立一套準則用以決定誰是下一個接收信息的交易參加者或是下一個接收信息的路由器。

一個路由器就是一個閘道器/渠道，是由前一個層次(previous level)收集各個信息且把收到的所有信息依據SP的要求條件做一些資料處理，例如把從不同層次源所收集到之信息做合併之後轉傳給SP。每一個交易參加者只需製作自己的信息(意指格式化數據及加附電子簽章)後傳送至下一個層次。一個交易參加者先把所有已收到的信息與自己所製作的信息做合併形成聯合信息，然後把聯合信息

(請先閱讀背面之注意事項再填寫本頁)

訂

線

五、發明說明 (57)

做電子簽章後傳至鄰接層次。在職階式組織排列中最簡單的排列方法是，僅有一個路由器把所有其他交易參加者的信息收集一起形成聯合信息之後傳給SP。

在串聯排列方式中，一個交易源始者是與所有路由器及/或所有交易參加者做串聯式的交易路徑排列，串聯後的所有路由器及/或所有交易參加者再接著再與SP做串聯式的交易路徑排列。在本發明較佳具體例中，每一個構成分子正是代表一個交易參加者；本發明另一個具體例中，居於交易源始者與SP之間的中間構成分子可以是一個路由器。

一個交易源始者與複數個交易參加者100, 1120, 1140, 及1160及一個SP執行一個電子交易，如第12圖所示，第12圖與第6A至6Q圖中所描述之三個參加單位(three party)行動方案是相類似，只不過第12圖是含及較多的交易參加者；交易參加者3、4、5、6...n-2是以串聯方式排列，每一個交易參加者把自己製做好的信息與前一個交易參加者傳送來的信息做合併，意指如果有前一個交易參加者傳送來信息的話，然後所合併之信息加附一個電子簽章形成聯合信息後傳至路徑上的鄰接交易參加者；一個最終聯合要求信息會傳至SP，SP於是製作一個聯合回覆信息，SP按照聯合要求信息本來所行徑至SP的路徑再把SP聯合回覆信息傳至交易參加者們。

第13圖展示構成分子做成一個職階式組織排列方案，第13圖中每一個構成分子 $X_{1,1}$ 至 $X_{1,n}$ $X_{j,k}$ 1200($n=1, 2$

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

90. 12. 11 修正
年 月 日 補充

A7
B7

五、發明說明 (58)

，3...)是一個交易參加者而不是一個路由器，每一個構成分子 $X_{j,k}$ 1210 ($j=2, 3, 4, \dots$; $k=1, 2, 3, \dots, m$; m 是一個 n 類型(type)的變數，在不同的職階層次中 m 可以是不同的值)的身分可以是一個交易參加者或是一個路由器兩者中之任何一者。箭頭向上的符號代表傳送一個交易要求信息1220，箭頭向下的符號代表傳送一個交易回覆信息1230。

每一個交易參加者把其所負責收集的若干的交易參加者之信息，與其自己所製作的信息做合併形成一個新的信息後把該新的信息傳至鄰接層次，職階組織排列方案可以含及多達交易所需之交易參加者數目(職階式組織方案中最簡化的情況(case)是一個交易參加者與一個SP進行之交易)，至最終時，SP之前面一個層次裏的最後一個結構分子 $X_{\sigma,k}$ ， σ 是一個種類 n ，把各路徑所傳來的的信息均合併形成一個信息1240後傳至SP 60，同樣地，SP製作回覆信息後SP把回覆信息按原先傳來之路徑傳回。

在SP不全程主導第一及第二階段的情況時，會員們是用SP所產製與配發的期間密鑰於第二階段進行相互間的交易，SP不全程主導第一及第二階段的情況時，可有二個至二個以上的會員參加交易。當有二個以上的會員們相互間使用時段交易所進行的交易時，信息由一個會員傳至另一個會員是可以任何順序做傳遞；某甲會員使用期間密鑰把一個要求交易信息做加密後傳至某乙會員時，某乙會員會也使用相同一個期間密鑰把交易回覆信息做加密後

五、發明說明 (59)

再回傳給某甲會員。某A會員把信息傳至某B會員之後某B會員要回覆給某A會員的回覆信息不一定就要由某B會員處直接發送回給某A。例如一個組織成環狀(ring)的三個會員們的(使用期間密鑰做信息加密)電子交易中，可以順時鐘繞著環狀的方向進行交易；例如一個會員甲、乙、及丙相互間的(使用期間密鑰)電子交易中：甲傳一個要求信息至乙，乙傳一個要求信息及一個回覆信息至丙，丙傳一個要求信息及一個回覆信息至甲，甲傳一個回覆信息至乙。乙接收到甲的交易要求信息後會製做一個回覆給甲的交易回覆信息，該個交易回覆信息不論是依照怎樣的行徑順序做傳遞最終還是會被傳至甲。

在SP不全程主導第一及第二階段的情況時，其於金鑰換階段中SP已接收到所有各個參加交易會員們的每一把公開金鑰；在會員們相互間用時段交易所進行的交易之前，SP會把其他參加會員們的每一把公開金鑰全部傳給每一個參加交易的會員。會員間送訊之前所製作交易要求信息及交易回覆信息有含及送訊端的明文--意思是指如果有明文的話、送訊端的一個密文、及送訊端的一個電子簽章。

當SP需要與例如以EC持卡人電子憑證代理人身分及商家的電子憑證代理人身分去與以電子憑證為交易機制的外界系統1080進行交易或是做資訊交換時，SP是EC持卡人及商家與外界操作介面間的鎧甲，SP只會把EC持卡人及商家所需要用以完成與外界系統做交易的資訊經SP做交

五、發明說明 (60)

換後轉傳給EC持卡及商家。

視為本發明之較佳具體例子至此處已是經過完整詳細說明及附圖描述；就拿技術中之一般性技巧而言本發明之一些其他變更也是很清楚的，因此，所想要做的就是確保在本發明申請專利範圍之附加項目中(appended claims)，把所有諸如本發明之變更及本發明之延伸均落實在本發明之真正精神及發明範圍內。本發明之構建含及所有具體例子，由是均落實於本發明申請專利範圍之附加項目內，且本發明只應被限制在以下所列載申之請專利範圍之附加項目中。此外，對擁有技術中之一般性技巧者而言，會隨時分辨出那一些可以用來替代於此處所發表的其他的應用沒有悖離本發明之精神及發明範圍。

元件標號對照表

20 EC 卡持卡人	94 連結網路之介面裝置	132 明文
22 輸入/輸出介面裝置	102 電腦	134 生成 EC 信息摘要
24 處理系統	104 電腦	136 電子簽章
30 EC 讀/寫卡器之介面裝置	106 電腦	138 讀取 EC 私密金鑰
40 商家終端電腦系統	108 交易機制	140 合併
50 網路	110 存取條件	142 裝備
60 服務提供者主機電腦系統	112 比較	144 挑選服務提供者
70 商家電腦端	114 通關存取條件資料	146 加密
72 EC 相等功能軟體	116 用卡要求被拒	148 亂數產生器
74 連結網路之介面裝置	118 被開啟使用	150 讀取商家公開金鑰
82 EC 讀/寫卡器之介面裝置	120 讀取 SP 公開金鑰	152 敏感性交易數據
84 EC 卡持卡人之個人電腦	122 加密	154 合併
86 輸入/輸出介面裝置	124 亂數產生器	156 商家明文
88 連結網路之介面裝置	126 讀取 EC 公開金鑰	158 合併
90 顧客個人電腦端	128 敏感性交易數據	160 輸入單向雜湊演算法
92 EC 相等功能軟體	130 合併	162 電子簽章

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明 (61)

164 讀取商家私密金鑰	232(4)解密	302 讀取商家私密金鑰
166 合併	234 比較	304 合併
168 分離	236 廢棄	306 商家信息
170 解密	238 解密	306(1) 驗證
172 比較	240 比較	306(2) 分離
174 廢棄	242 廢棄	306(3) 商家準信息摘要
176 分離及解密	244 加密器	306(4) 分離
178 比較	246 亂數	308 廢棄
180 廢棄	248 帳戶資料	310 解密
182 加密	250 商家敏感性數據	312 比較
184 亂數產生器	252 交易價金	314 廢棄
186 期間密鑰	254 合併	316 步驟
188 EC 亂數	256 交易辨識碼	318 驗證
190 敏感性交易數據	258 商家明文	320 廢棄
192 合併	260 商家信息	322 分離
194 交易辨識碼	260(1) 分離	324 解密
196 明文	260(2) 分離	326 步驟
198 信息摘要	260(3) 解密	328 廢棄
200 電子簽章	262 比較	330 解密
202 讀取 SP 私密金鑰	264 廢棄	332 比較
204 合併	266 解密	334 廢棄
206 加密	268 步驟	336 加密
208 亂數產生器	270 廢棄	338 交易回應數據
210 期間密鑰	272 加密	340 合併
212 商家亂數	274 亂數	342 交易辨識碼
214 敏感性交易數據	276 帳戶資料	344 明文
216 合併	278 敏感性數據	346 生成電子簽章
218 交易辨識碼	280 交易價金	348 電子簽章
220 明文	282 合併	350 讀取 SP 私密金鑰
222 合併	284 交易辨識碼	352 合併
224 生成信息摘要	286 明文	354 加密
226 電子簽章	288 生成信息摘要	356 交易回應數據
228 讀取 SP 私密金鑰	290 電子簽章	358 合併
230 合併	292 讀取 EC 私密金鑰	360 交易辨識碼
232 商家信息	294 合併	362 明文
232(1)分離	296 合併	364 商家信息之數據部份
232(2)單向雜湊演算法	298 生成商家信息摘要	366 電子簽章
232(3)分離	300 電子簽章	368 電子簽章

(請先閱讀背面之注意事項再填寫本頁)

裝
訂
線

五、發明說明 (62)

- 370 讀取 SP 私密金鑰

372 合併

374 商家信息

374(1) 檢查

374(2) 分離

374(3) 輸入

374(4) 分離

376 廢棄

378 解密

380 比較

382 廢棄

384 加密

386 交易數據

388 合併

390 交易辨識碼

392 明文

394 EC 信息

394(1) 檢查

394(2) 分離

394(3) 生成準信息摘要

394(4) 分離

396 廢棄

398 EC 信息

400 比較

402 廢棄

404 加密

406 交易數據

408 合併

410 交易辨識碼

412 明文

414 生成信息摘要

416 電子簽章
- 418 讀取 EC 私密金鑰

420 合併

422 合併

424 生成信息摘要

426 電子簽章

428 讀取商家私密金鑰

430 合併

432 商家信息

432(1) 驗證

432(2) 分離

432(3) 生成準信息摘要

432(4) 分離

434 廢棄

436 解密

438 比較

440 廢棄

442 解密

444 EC 信息

444(1) 分離

444(2) 生成準信息摘要

444(3) 分離

446 解密

448 比較

450 廢棄

452 解密

454 交易完成

500 記憶體

550 電子卡操作系統

600 存取條件

650 密碼服務供應器

700 服務提供者數據區

702 服務提供者名稱
- 704 金鑰種類

706 金鑰值

708 帳戶資料

710 卡種類 710

712 個人身分識別通關密碼

714 其他資料

750 EC 卡持卡人個人資料暨
複數個配對之公開金鑰/
私密金鑰

800 其他用途

900 送訊端訊息 M 之數據部
份*

902 單向雜湊演算法

903 $H(*)=MD$

904 電子簽章

906 送訊端訊息 M 之數據部
份*

908 解密後復原 MD

909 信息摘要

910 單向雜湊演算法

911 $H(*)=MD^{\wedge}$

912 電子簽章

1000、1020、1040、1060、
1080 外界系統

1100、1120、1140、1160、1180
複數個交易參加者

1200 構成分子

1210 構成分子

1220 交易要求信息

1230 交易回覆信息

1240 信息

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

四、中文發明摘要 (發明之名稱： 電子交易用密碼系統與方法)

一種執行交易各參加單位間之安全電子交易系統共合及各電子卡持卡人、各商家們及各服務提供者。本系統所合及之電子卡就是眾所周知的各類智慧卡，及具各類智慧卡相等功能暨實效之軟體，該等卡是去模仿真正錢包，包括模仿各種信用卡、支票簿或駕駛執照等等平常所見之金融性或非金融性載具。該等卡通常是經由公開網路例如網際網路使用混合式密碼系統去執行電子交易。使用複數個亂數與複數個電子簽章以確保所有參加交易單位間所傳送之資料的真實性暨有效性。使用對稱性密秘金鑰密碼系統例如服務提供者們 (SPs) 所產製定並指定分配給各電子卡及各商家之期間密鑰以確保每一交易之隱私性，僅有 SP (接下頁)

英文發明摘要 (發明之名稱： A CRYPTOGRAPHIC SYSTEM AND METHOD FOR ELECTRONIC TRANSACTIONS)

An electronic transaction system, which facilitates secure electronic transactions among multiple parties including cardholders, merchants, and service providers (SP). The system involves electronic cards, commonly known as smart cards, and their equivalent computer software package. The card mimics a real wallet and contains commonly seen financial or non-financial instruments such as a credit card, checkbook, or driver license. A transaction is protected by a hybrid key cryptographic system and is normally carried out on a public network such as the Internet. Digital signatures and random number are used to ensure integrity and authenticity. The card utilizes secret keys such as session keys assigned by service providers (SPs) to ensure privacy for each transaction. The SP is solely responsible for validating each participant's sensitive information and assigning session keys. The system does not seek to establish a trust relationship between two participants of a transaction. The only trust relationship needed in a transaction is the one that exists between individual participants and the SP. The trust relationship with a participant is established when the SP has received and validated certain established account information from that particular participant. To start a transaction with a selected SP, a participant must have the public key of the intended SP. Since the public key is openly available, its availability can be easily established by the cardholder. The SP also acts as a gateway for the participants when a transaction involves interaction with external systems.

(請先閱讀背面之注意事項再填寫本頁各欄)

裝

訂

四、中文發明摘要 (發明之名稱：

(承上頁)

才能驗證各交易參加者之敏感性資料及製發期間密鑰。本系統不主張於一個交易中去建立任何兩造間的電子憑證互信式關係，在本系統交易中唯一需要的是交易之前就已存在於各個交易參加者與 SP 之間的會員式互信關係。SP 收到某一位會員之信息後，當 SP 對該會員之一些建檔帳戶資料執行驗證為有效會員時，此刻 SP 與該會員之線上互信就建立。一個會員必需要持有其意欲使用之 SP 的公開金鑰才能開始與之交易，正因公開金鑰是公諸於世所以電子卡持卡人是容易就可得到並安裝於卡上。當會員涉及與外界系統做相互接觸時，SP 是擔任其各個參加交易會員與外界系統間的一個開道器。

英文發明摘要 (發明之名稱：

(請先閱讀背面之注意事項再填寫本頁各欄)

裝

訂

線

四、中文發明摘要 (發明之名稱： 電子交易用密碼系統與方法)

一種執行交易各參加單位間之安全電子交易系統共含及各電子卡持卡人、各商家們及各服務提供者。本系統所
含及之電子卡就是眾所周知的各類智慧卡，及具各類智慧
卡相等功能暨實效之軟體，該等卡是去模仿真正錢包，包
括模仿各種信用卡、支票簿或駕駛執照等等平常所見之金
融性或非金融性載具。該等卡通常是經由公開網路例如網
際網路使用混合式密碼系統去執行電子交易。使用複數個
亂數與複數個電子簽章以確保所有參加交易單位間所傳送
之資料的真實性暨有效性。使用對稱性密秘金鑰密碼系統
例如服務提供者們(SPs)所產製定並指定分配給各電子卡
及各商家之期間密鑰以確保每一交易之隱私性，僅有SP
(接下頁)

英文發明摘要 (發明之名稱： A CRYPTOGRAPHIC SYSTEM AND METHOD FOR)
ELECTRONIC TRANSACTIONS

(請先閱讀背面之注意事項再填寫本頁各欄)

裝

訂

四、中文發明摘要 (發明之名稱：)

(承上頁)

才能驗證各交易參加者之敏感性資料及製發期間密鑰。本系統不主張於一個交易中去建立任何兩造間的電子憑證互信式關係，在本系統交易中唯一需要的是交易之前就已存在於各個交易參加者與 SP之間的會員式互信關係。SP收到某一位會員之信息後，當SP對該會員之一些建檔帳戶資料執行驗證為有效會員時，此刻SP與該會員之線上互信就建立。一個會員必需要持有其意欲使用之SP的公開金鑰才能開始與之交易，正因公開金鑰是公諸於世所以電子卡持卡人是容易就可得到並安裝於卡上。當會員涉及與外界系統做相互接觸時，SP是擔任其各個參加交易會員與外界系統間的一個開道器。

英文發明摘要 (發明之名稱：)

(請先閱讀背面之注意事項再填寫本頁各欄)

裝

訂

線

90年12月1日

修正
補充A8
B8
C8
D8

六、申請專利範圍

第88119209號申請案申請專利範圍修正本 90.12.11.

1. 一種電子交易系統，包括
 - 一個電子卡(electronic card, EC)，具有：
 - 一個密碼器種類服務區可選擇密碼器做執行加密及解密；
 - 一個數據區用以儲存資料；及
 - 一個數據區用以儲存持卡人與服務提供者會員終端機(service provider member terminal)間之數據；
 - 一個服務提供者會員終端機會對電子卡之要求做出回應；及
 - 一個服務提供者終端機(service provider terminal)通聯至服務提供者會員終端機。
2. 如申請專利範圍第1項之系統，其中該電子卡是一個具有實質外形之卡片。
3. 如申請專利範圍第1項之系統，進一步包括使用與電子卡具有相等功能暨實效之電腦軟體。
4. 如申請專利範圍第1項之系統，其中該電子卡進一步包括一個控卡操作系統執行安裝及更新持卡人卡上資料，持卡人變更通關密碼PIN，及管理服務提供者數據區。
5. 如申請專利範圍第1項之系統，其中該電子卡執行卡與外界之讀/寫通訊作業，及通訊協定處置。
6. 如申請專利範圍第1項之系統，其中該電子卡進一步包括一個管理電子卡之電腦軟體。

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

六、申請專利範圍

7. 如申請專利範圍第1項之系統，其中儲存服務提供者資料之數據區包括一個服務提供者記錄(record)，該記錄包括：
 - 一個服務提供者名稱區域用以顯示服務提供者名稱；
 - 一個金鑰值區域；及
 - 一個帳戶資料區域，該區所含及之資料對每一位服務提供者而言是獨有。
8. 如申請專利範圍第1項之系統，其中電子卡進一步包括應用電腦軟體。
9. 如申請專利範圍第1項之系統，其中電子卡進一步包括爪哇獨立作業applet電腦軟體。
10. 如申請專利範圍第1項之系統，進一步包括外界系統，其中服務提供者終端系統與外界系統做通聯。
11. 如申請專利範圍第7項之系統，其中每一個服務提供者記錄(record)進一步包括卡種類區域用以指明該個服務提供者所支援之載具種類(type of instrument)。
12. 一種使用電子卡執行電子交易之方法，其步驟包括：
 - 於服務提供者端產製一把期間密鑰；
 - 金鑰交換是從一個會員傳送一把金鑰至服務提供者，及從服務提供傳送一把期間密鑰至該會員；及
 - 用該期間密鑰去執行一個交易。
13. 如申請專利範圍第12項之方法，其中在金鑰交換階段中之步驟，包括：

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

90年12月1日 修正
補充

六、申請專利範圍

從一個會員傳送一個金鑰交換要求信息至服務提供者；及

服務提供者格式化一個金鑰交換回覆信息，該信息含及指定傳送給該會員所使用之期間密鑰並傳送該金鑰交換回覆信息至該會員。

14. 如申請專利範圍第12項之方法，其中使用期間密鑰之步驟去執行一個交易之複數個步驟，包括：

使用期間密鑰去格式化一個會員交易要求信息並把該會員交易要求信息傳送至服務提供者；及

服務提供者格式化一個回覆給該會員之交易回覆會員信息並把交易回覆會員信息傳至該會員。

15. 如申請專利範圍第12項之方法，其中使用期間密鑰之複數個步驟去執行一個交易之複數個步驟，包括：

第一個會員使用期間密鑰格式化一個交易要求信息，該交易要求信息含及一個第一個會員之電子簽章，及把該交易要求信息傳至第二個會員；以及

第二個會員使用期間密鑰格式化一個交易回覆信息，該交易回覆信息含及一個第二個會員之電子簽章，及把該交易回覆信息傳至第一個會員。

16. 如申請專利範圍第12項之方法，其中使用期間密鑰之步驟去執行一個交易之複數個步驟，包括：

第一個會員使用期間密鑰格式化一個交易要求信息，該交易要求信息含及一個第一個會員之電子簽章，及把該交易要求信息傳至一個中間會員(intermediate

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

六、申請專利範圍

member)；以及

該中間會員使用期間密鑰格式化一個交易回覆信息，該交易回覆信息含及一個該中間會員之電子簽章，及把該交易回覆信息傳至一個最尾端(final)會員；

該最尾端會員使用期間密鑰格式化一個交易回覆信息，該交易回覆信息含及一個該最尾端會員之電子簽章，及把該交易回覆信息傳至該第一個會員。

17. 如申請專利範圍第12項之方法，其中交換金鑰階段之步驟包括複數個步驟：

電子卡傳送一個電子卡金鑰交換要求信息至一個商家終端機；

商家終端機把商家金鑰交換要求信息與電子卡金鑰交換要求信息做合併形成一個電子卡-商家最終聯合換鑰要求信息，及把電子卡-商家最終聯合換鑰要求信息傳至一個服務提供者；

服務提供者格式化一個服務提供者換鑰回覆商家信息含及一個服務提供者給商家之服務提供者期間密鑰，服務提供者格式化一個服務提供者換鑰回覆電子卡信息含及一個服務提供者給電子卡之服務提供者期間密鑰，服務提供者把服務提供者換鑰回覆商家信息與服務提供者換鑰回覆電子卡信息做合併形成一個服務提供者聯合換鑰回覆電子卡-商家信息，及把服務提供者聯合換鑰回覆電子卡-商家信息傳至商家終端機；以及

商家終端機把服務提供者換鑰回覆商家信息與服

六、申請專利範圍

務提供者換鑰回覆電子卡信息做分離，及商家終端機把服務提供者換鑰回覆電子卡信息轉傳至電子卡。

18. 如申請專利範圍第12項之方法，其中使用期間密鑰之步驟去執行一個交易之複數個步驟，包括；

電子卡使用期間密鑰格式化一個電子卡交易要求信息並把該交易要求信息傳至商家終端機；

商家終端機使用期間密鑰式化一個商家終端機交易要求信息，商家終端機把商家終端機交易要求信息與所收到的電子卡交易要求信息做合併形成一個電子卡-商家終端機最終聯合交易要求信息，及商家終端機再把電子卡-商家終端機最終聯合交易要求信息傳至服務提供者；

服務提供者使用期間密鑰式化一個交易回覆商家終端機信息用以回答商家終端機，服務提供者使用期間密鑰式化一個交易回覆電子卡信息用以回答電子卡，服務提供者把一個交易回覆商家終端機信息與一個交易回覆電子卡信息做合併形成一個最終聯合交易回覆電子卡-商家終端機信息，及服務提供者再把最終聯合交易回覆電子卡-商家終端機信息傳至商家終端機；以及

商家終端機把所接收到的最終聯合交易回覆電子卡-商家終端機信息傳做分離，商家終端機取得交易回覆商家終端機信息及交易回覆電子卡信息，及商家終端機把交易回覆電子卡信息轉傳至電子卡。

19. 如申請專利範圍第12項之方法，其中服務提供者是全程

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

六、申請專利範圍

主導金鑰交換階段及交易階段時，每一個會員所傳送之信息中有含及敏感性交易數據時僅有服務提供者才能讀取該敏感性交易數據。

20. 如申請專利範圍第12項之方法，其中服務提供者只主導金鑰交換階段但不主導交易階段時，金鑰交換階段中每一個會員所傳送之信息中有含及敏感性交易數據時僅有服務提供者才能讀取該敏感性交易數據。

21. 如申請專利範圍第13項之方法，其中金鑰交換回覆交易信息中進一步含及涉及一個電子交易中之每一位交易參加者之公開金鑰。

22. 如申請專利範圍第13項之方法，其中金鑰交換交易要求信息中之密文部份含及一個會員所生成之亂數。

23. 如申請專利範圍第13項之方法，其中金鑰交換交易要求信息中含及一個會員所生成之電子簽章。

24. 如申請專利範圍第13項之方法，其中一個會員所傳送之金鑰交換信息中含及一個密文，該密文包括：

一個會員亂數；及

該會員之敏感性數據。

25. 如申請專利範圍第14項之方法，其中交易信息中之密文部份含及一個亂數。

26. 如申請專利範圍第14項之方法，其中交易信息中含及一個送訊端之電子簽章。

27. 如申請專利範圍第14項之方法，其中交易信息中有含及敏感性交易數據時僅有服務提供者才能讀取該敏感性

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

90年12月1日

修正
補充A8
B8
C8
D8

六、申請專利範圍

交易數據。

28. 如申請專利範圍第14項之方法，進一步包括複數個步驟：

會員使用期間密鑰格式化一個承認交易信息並把該承認交易信息傳至服務提供者。

29. 如申請專利範圍第18項之方法，進一步包括複數個步驟：

電子卡使用期間密鑰格式化一個電子卡承認交易信息並把該承認交易信息傳至商家終端機；及

商家終端機使用期間密鑰格式化一個商家終端機承認交易信息，商家終端機把商家終端機承認交易信息與所收到的電子卡承認交易信息做合併形成一個電子卡-商家終端機最終聯合承認交易信息，接著商家終端機再把電子卡-商家終端機最終聯合承認交易信息傳至服務提供者。

30. 如申請專利範圍第24項之方法，其中金鑰交換要求信息進一步包括明文。

31. 如申請專利範圍第24項之方法，其中金鑰交換要求信息進一步包括一個會員之電子簽章。

32. 如申請專利範圍第24項之方法，其中密文進一步包括一個會員之公開金鑰。

33. 如申請專利範圍第25項之方法，其中一個交易信息進一步包括一個送訊端之電子簽章。

34. 一種傳送金鑰交換信息之方法，包括下列步驟：

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

六、申請專利範圍

電子卡持卡人符合電子卡各項存取條件；

電子卡持卡人挑選一個服務提供者；

電子卡產製一個電子卡亂數；

電子卡使用服務提供者公開金鑰把一個電子卡亂數、一個電子卡公開金鑰、及電子卡敏感性交易數據做加密形成一個電子卡密文；

如果電子卡有明文時，電子卡把電子卡密文與電子卡明文做合併形成一個電子卡換鑰要求信息之數據部份；

電子卡把電子卡換鑰要求信息之數據部份輸入一個單向雜湊函演算法生成一個電子卡信息摘要；

電子卡使用電子卡私密金鑰把電子卡信息摘要做簽章形成一個電子卡電子簽章；

電子卡把電子卡換鑰要求信息之數據部份與電子卡電子簽章做合併形成一個電子卡換鑰要求信息；及

經一個網路，電子卡把電子卡換鑰要求信息傳至一個商家。

35. 如申請專利範圍第34項之方法，進一步包括下列步驟：

商家裝置產製一個商家亂數；

商家裝置使用服務提供者公開金鑰把一個商家亂數、一個商家公開金鑰、及商家敏感性交易數據做加密形成一個商家密文；

如果商家有明文時，商家把商家密文與商家明文做合併形成一個商家換鑰要求信息之數據部份；

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

90.12.14

修正

補充

六、申請專利範圍

商家裝置把電子卡換鑰要求信息與商家換鑰要求信息之數據部份做合併形成一個電子卡-商家最終聯合換鑰信息之數據部份；

商家裝置把電子卡-商家最終聯合換鑰信息之數據部份輸入一個單向雜湊函演算法生成一個商家信息摘要；

商家裝置使用商家私密金鑰把商家信息摘要做簽章形成一個商家電子簽章；

商家把電子卡-商家最終聯合換鑰信息之數據部份與商家電子簽章做合併形成一個電子卡-商家最終聯合換鑰要求信息；及

經一個網路商家把電子卡-商家最終聯合換鑰要求信息傳至一個服務提供者。

36. 一種金鑰交換要求信息，包括：

電子卡明文；

用一個服務提供者公開金鑰做加密之電子卡密文中，包括一個電子卡亂數，一把電子卡公開金鑰，及電子卡敏感性數據；

電子卡明文與電子卡密文做簽章形成之一個電子卡電子簽章；

商家明文；

用一個服務提供者公開金鑰做加密之密文中，包括一個商家亂數，一把商家公開金鑰，及商家敏感性數據；及

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

六、申請專利範圍

商家明文與商家密文做簽章形成之一個商家電子簽章。

37. 一種金鑰交換回覆信息，包括：

服務提供者(SP)要傳送給EC之SP-EC明文；

SP產製並指定傳送給電子卡之SP-EC交易辨識碼；

用一把EC公開金鑰做加密之SP-EC密文中含有一個EC亂數，一個SP-EC亂數，一把SP要傳給EC之期間密鑰，及SP要傳給EC之SP-EC敏感性數據；

一個SP-EC電子簽章中含有SP要傳給EC之SP-EC明文，SP要傳給EC之SP-EC易識別碼，SP要傳給EC之SP-EC密文；

SP要傳給商家之SP-商家明文；

SP產製並指定傳送給商家之SP-商家交易辨識碼；

用一把商家公開金鑰做加密之SP-商家密文中含有一個商家亂數，一個SP-商家亂數，一把SP要傳給商家之期間密鑰，及SP要傳給商家之SP-商家敏感性數據；
及

一個SP-商家電子簽章中含有SP要傳給商家SP-商家明文，與SP要傳給商家SP-商家交易識別碼，與SP要傳給商家SP-商家密文。

38. 一種用於排成串列形態之複數個單位(parties)參加者間執行電子交易之方法，其步驟包括：

從電子卡傳送一個電子卡金鑰交換要求信息至第一單位(first party)，該第一單位是一個信息路由器或是

90. 12. 1

修正
補充A8
B8
C8
D8

六、申請專利範圍

一個交易參加者；

如果第一單位只是一個信息路由器時，從第一單位傳送一個金鑰交換要求信息至一個鄰接單位(next party)；

如果第一單位是一個交易參加者時，第一單位把第一單位金鑰交換要求信息與電子卡金鑰交換要求信息做合併形成一個電子卡-第一單位聯合金鑰交換要求後信息傳送至一個鄰接單位；

如果當時單位(current party)只是一個信息路由器時，當時單位把所接收到之金鑰交換要求信息轉傳至下一個鄰接單位；

如果當時單位是一個交易參加者時，當時單位把當時單位金鑰交換要求信息與前一單位(last party)之金鑰交換要求信息做合併形成一個聯合金鑰交換(換鑰)要求信息後傳送至一個鄰接單位；

對於每一個交易參加者，服務提供者均會為其格式化一個換鑰回覆信息，服務提供者按照聯合換鑰要求信息本來所行徑至服務提供者的路徑再把服務提供者最終聯合換鑰回覆信息傳至交易參加者們；及

每一個交易參加者把所屬於自己之換鑰回覆信息與屬於其他交易參加者們之換鑰回覆信息做分離，並按照聯合換鑰要求信息本來所行徑至服務供者的路徑再把屬於其他交易參加者們之換鑰回覆信息傳至交易參加者們，直到電子卡收到屬於於自己之交易回覆信息為

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

六、申請專利範圍

止。

39. 一種用於排成串列形態之複數個單位參加者間執行電子交易之方法，其步驟包括：

從電子卡傳送一個電子卡交易求信息至第一單位，該第一單位是一個信息路由器或是一個交易參加者 (participant)；

如果第一單位是一個信息路由器時，從第一單位傳送一個交易求要求信息至一個鄰接單位；

如果第一單位是一個交易參加者時，第一單位把第一單位交易要求信息與電子卡交易要求信息做合併形成一個電子卡-第一單位聯合交易要求信息後傳送至一個鄰接單位；

如果當時單位只是一個信息路由器時，當時單位把所接收到之交易要求信息轉傳至下一個鄰接單位；

如果當時單位是一個交易參加者時，當時單位把當時單位交易要求息與前一單位之交易要求信息做合併形成一個聯合交易要求後傳送至一個鄰接單位；

對於每一個交易參加者服務提供者均會為其格式化一個交易回覆信息，服務提供者按照聯合換鑰要求信息本來所行徑至服務提供者的路徑再把服務提供者最終聯合交易回覆信息傳至交易參加者們；及

每一個交易參加者把所屬於自己之交易回覆信息與屬於其他交易參加者們之交易回覆信息做分離，並按照聯合交易要求信息本來所行徑至服務供者的路徑再

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

12.11

修正
補充A8
B8
C8
D8

六、申請專利範圍

把屬於其他交易參加者們之交易回覆信息傳至交易參加者們，直到電子卡收到屬於於自己之交易回覆信息為止。

40. 一種用於使用職階式組織排列之複數個單位參加者間執行電子交易之方法，其步驟包括：

從電子卡傳送一個電子卡金鑰交換要求信息至第一單位(first party)，該第一單位是一個信息路由器或是一個交易參加者；

如果第一單位是一個信息路由器時，從第一單位傳送一個金鑰交換要求信息至一個鄰接單位(next party) $X_{j,k}$ ($j=2, 3, 4 \dots$; $k=1, 2, 3 \dots m$; m 是一個 n 類型(type)的變數，對於不相同的 j 值時 m 也可以是不相同的值)；如果第一單位是一個交易參加者時，第一單位把第一單位金鑰交換求信息與電子卡金鑰交換要求信息做合併形成一個電子卡-第一單位聯合金鑰交換要求信息後傳送至一個鄰接單位 $X_{j,k}$ ；

如果當時單位 $X_{j,k}$ 只是一個信息路由器時，當時單位 $X_{j,k}$ 把所接收到之交易要求信息轉傳至下一個鄰接單位 $X_{j,k}$ ；

如果當時單位 $X_{j,k}$ 是一個交易參加者時，當時單位把當時單位 $X_{j,k}$ 金鑰換要求信息與前一單位之金鑰交換要求信息做合併形成一個聯合金鑰交換(換鑰)要求信息後傳送至一個鄰接單位 $X_{j,k}$ ；

對於每一個交易參加者，服務提供者均會為其格式

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

六、申請專利範圍

化一個換鑰回覆信息，服務提供者按照聯合換鑰要求信息本來所行徑至服務提供者的路徑再把服務提供者最終聯合交易回覆信息傳至交易參加者們；及

每一個交易參加者把所屬於自己之交易回覆信息與屬於其他交易參加者們之交易回覆信息做分離，並按照聯合交易要求信息本來所行徑至服務供者的路徑再把屬於其他交易參加者們之交易回覆信息傳至交易參加者們，直到電子卡收到屬於於自己之交易回覆信息為止。

41. 一種用於使用職階式組織排列之複數單位參加者間執行電子交易之方法，其步驟包括：

從電子卡傳送一個電子卡交易求信息至第一單位，該第一單位是一個信息路由器或是一個交易參加者；

如果第一單位是一個信息路由器時，從第一單位傳送一個交易求要求信息至一個鄰接單位 $X_{j,k}$ ($j=2, 3, 4 \dots$; $k=1, 2, 3 \dots m$; m 是一個 n 類型 (type) 的變數，對於不相同的 j 值時 m 也可以是不相同的值) ；

如果第一單位是一個交易參加者時，第一單位把第一單位交易要求信息與電子卡交易要求信息做合併形成一個電子卡-第一單位交易要求後信息傳送至一個鄰接單位 $X_{j,k}$ ；

如果當時單位 $X_{j,k}$ 只是一個信息路由器時，該當時單位把所收到的交易要求信息轉傳至下一個鄰接單位

90.12.11

修正

A8
B8
C8
D8

六、申請專利範圍

$X_{j,k}$;

如果當時單位 $X_{j,k}$ 是一個交易參加者時，當時單位把當時單位 $X_{j,k}$ 交易要求信息與前一單位之交易要求信息做合併形成一個聯合交易要求信息後傳送至一個鄰接單位 $X_{j,k}$;

對於每一個交易參加者，服務提供者均會為其格式化一個交易回覆信息，服務提供者按照聯合換鑰要求信息本來所行徑至服務提供的路徑再把服務提供者最終聯合交易回覆信息傳至交易參加者們；及

每一個交易參加者把所屬於自己之交易回覆信息與屬於其他交易參加者們之交易回覆信息做分離，並按照聯合交易要求信息本來所行徑至服務供者的路徑再把屬於其他交易參加者們之交易回覆信息傳至交易參加者們，直到電子卡收到屬於於自己之交易回覆信息為止。

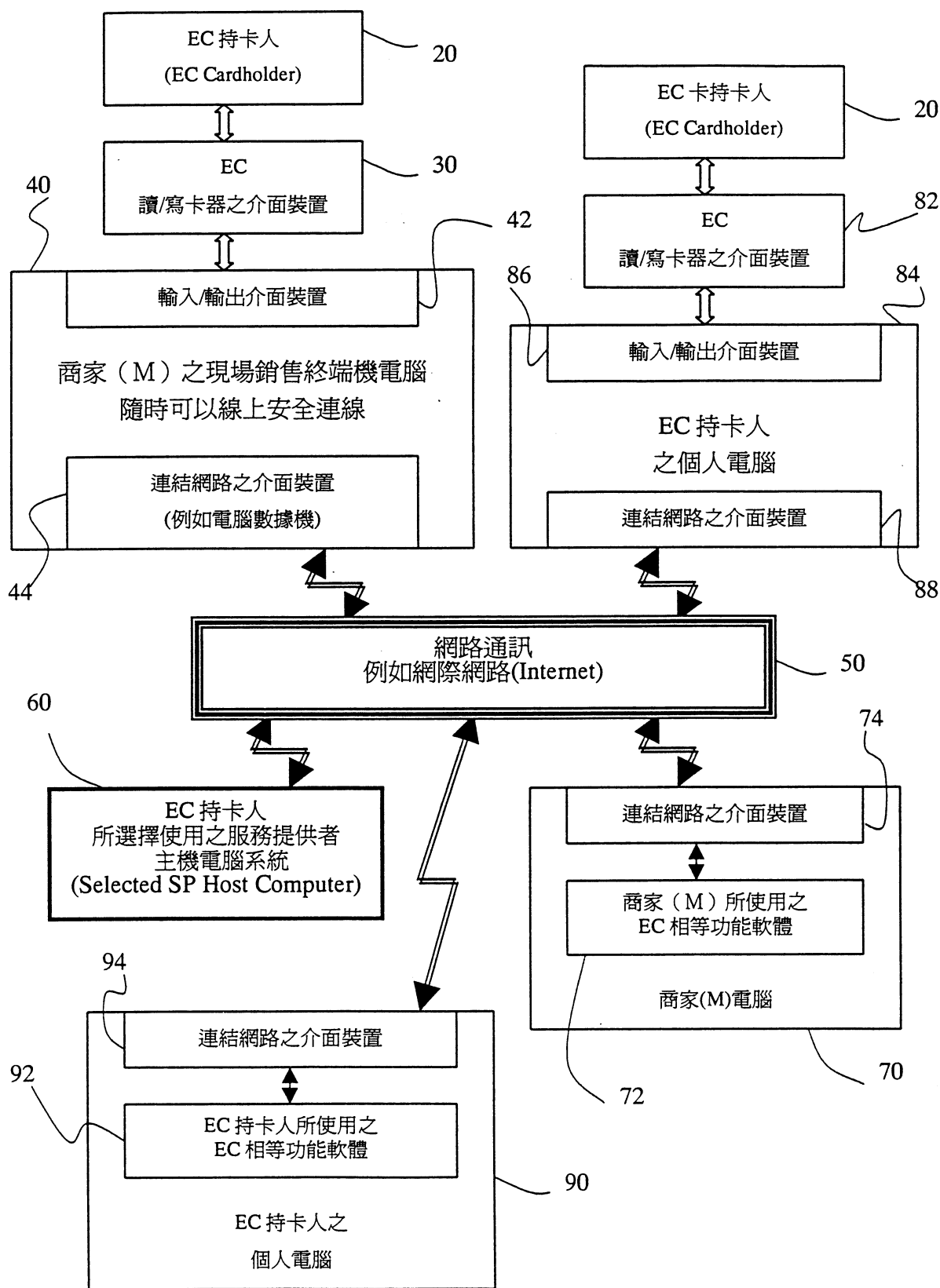
(請先閱讀背面之注意事項再填寫本頁)

裝

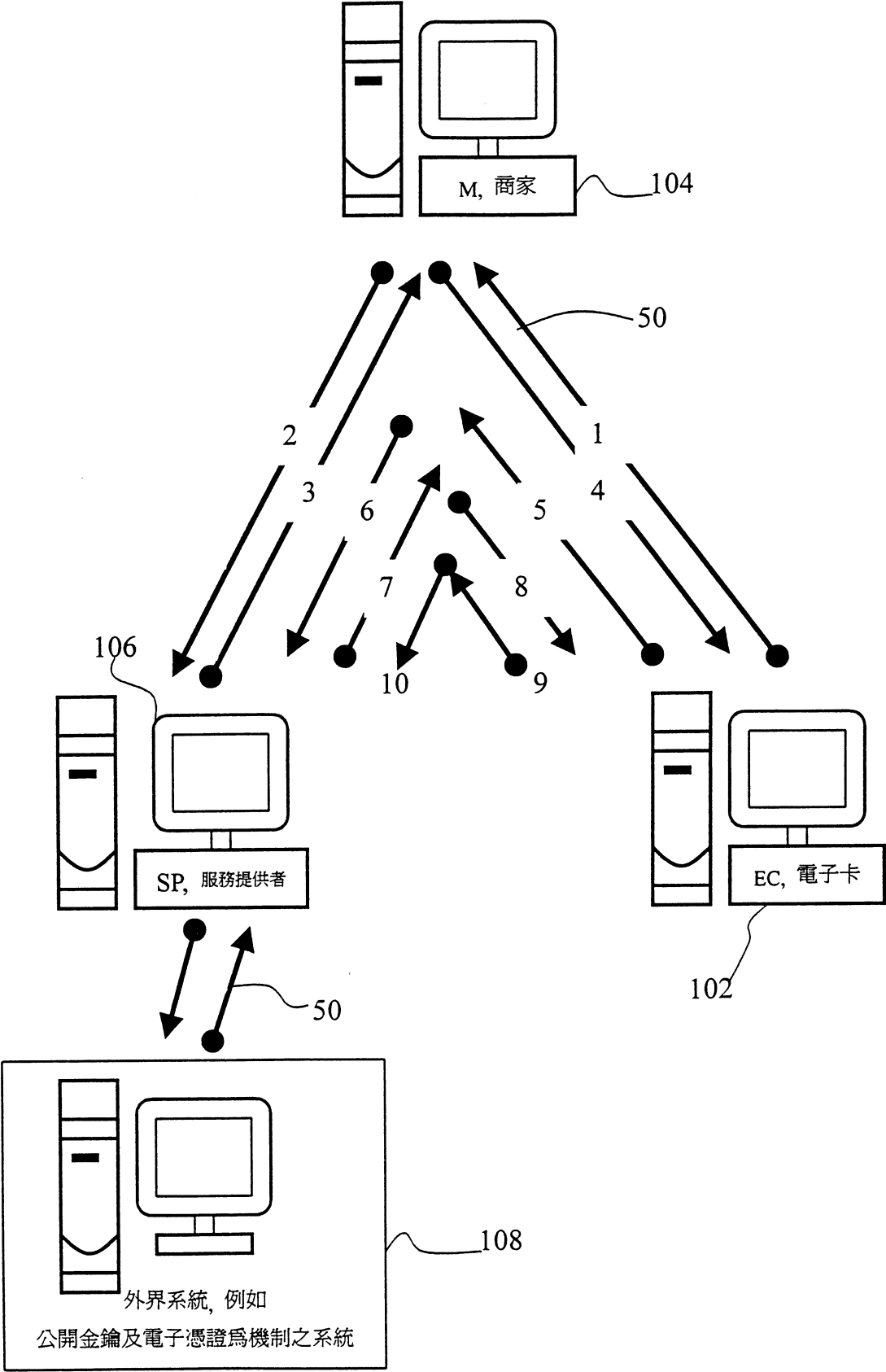
訂

線

第 1 圖



第 2 圖

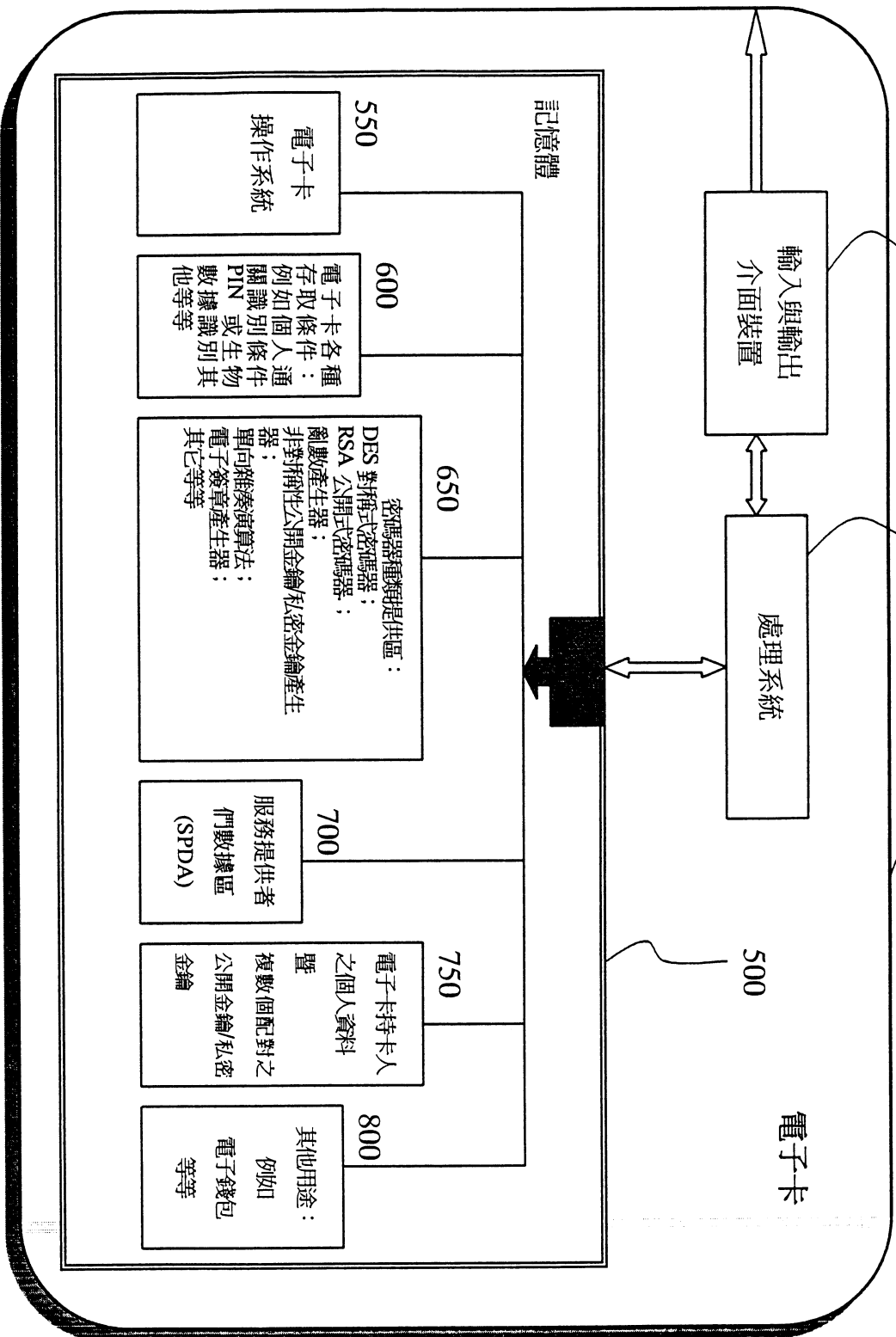


22

24

第 3 圖

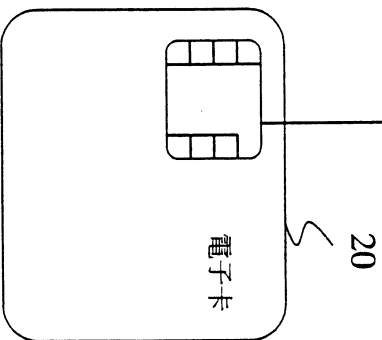
20



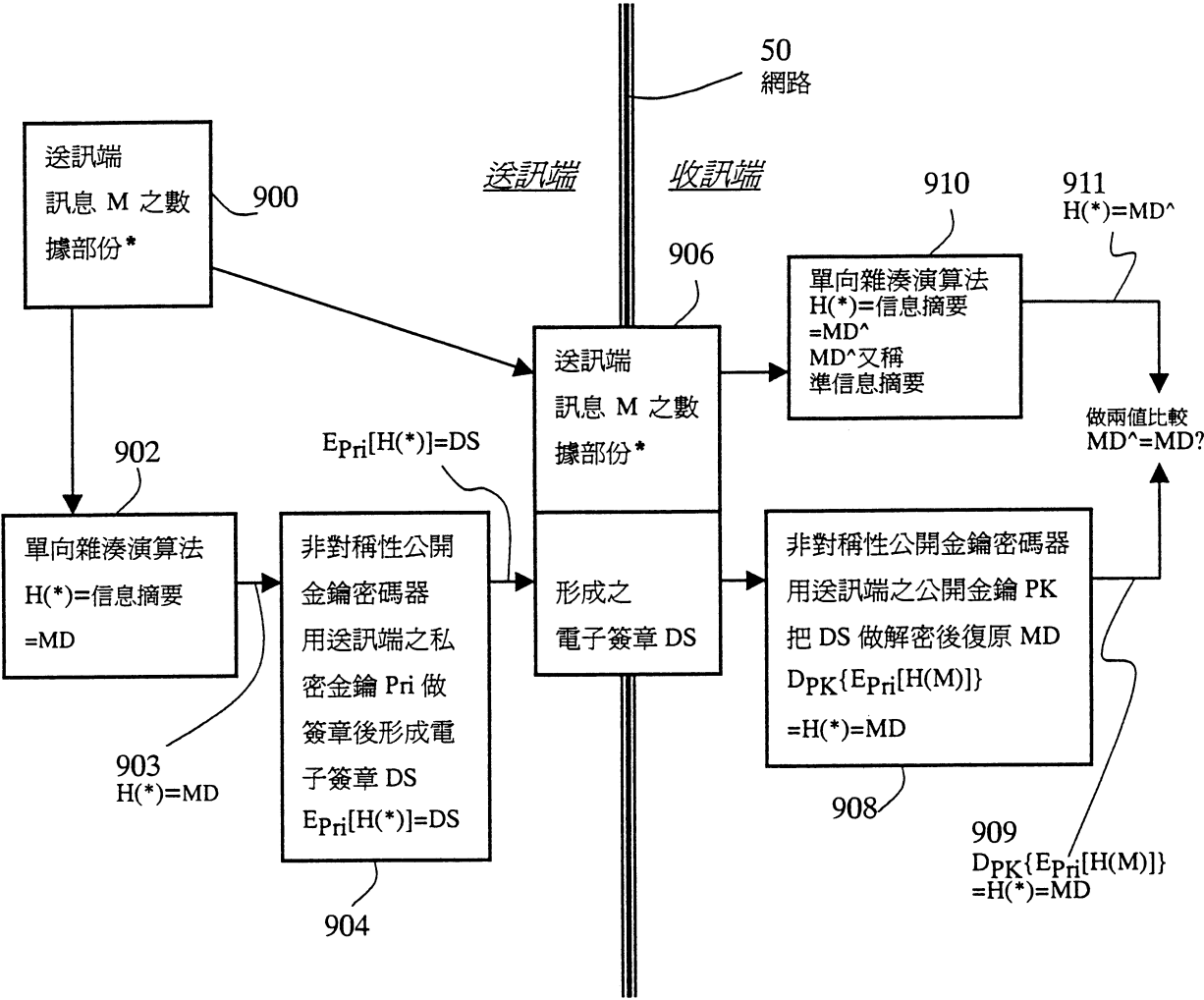
700

第 4 圖

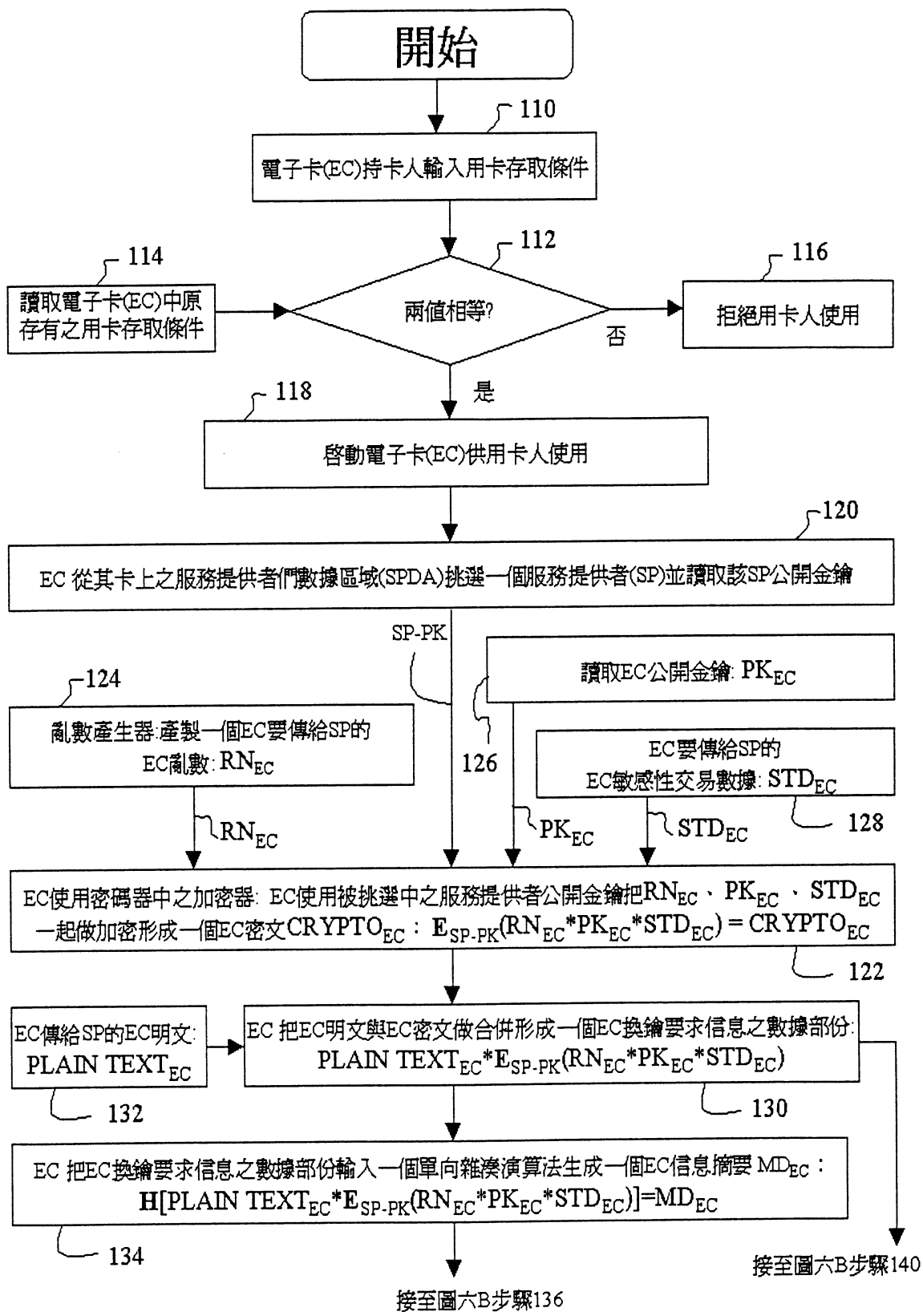
服務提供者們資料區 SERVICE PROVIDERS' DATA AREA (SPDA)						
702	704	706	708	710	712	714
服務提供者 之名稱	金鑰種類	金鑰值	SP 已核發給持卡人 之帳戶資料 (帳戶號碼，帳戶失效日期等等)	卡種類	個人通關識別密碼 PIN (可選擇或不選擇用 PIN)	其他 資料
				信用卡		
				轉帳卡		
				提款卡		
				會員卡		
				積分回饋 忠誠卡		
				其他 類別卡		



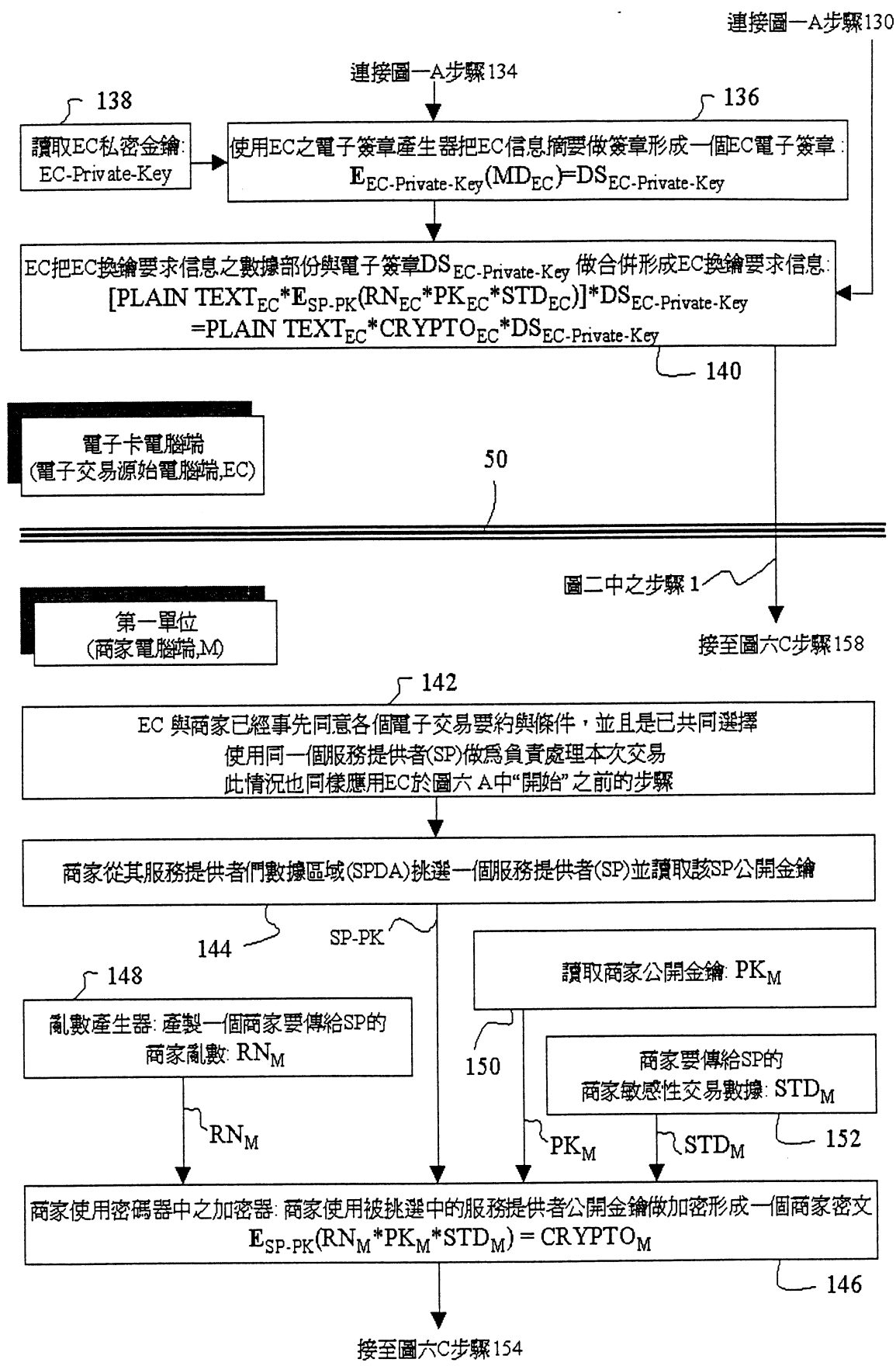
第 5 圖



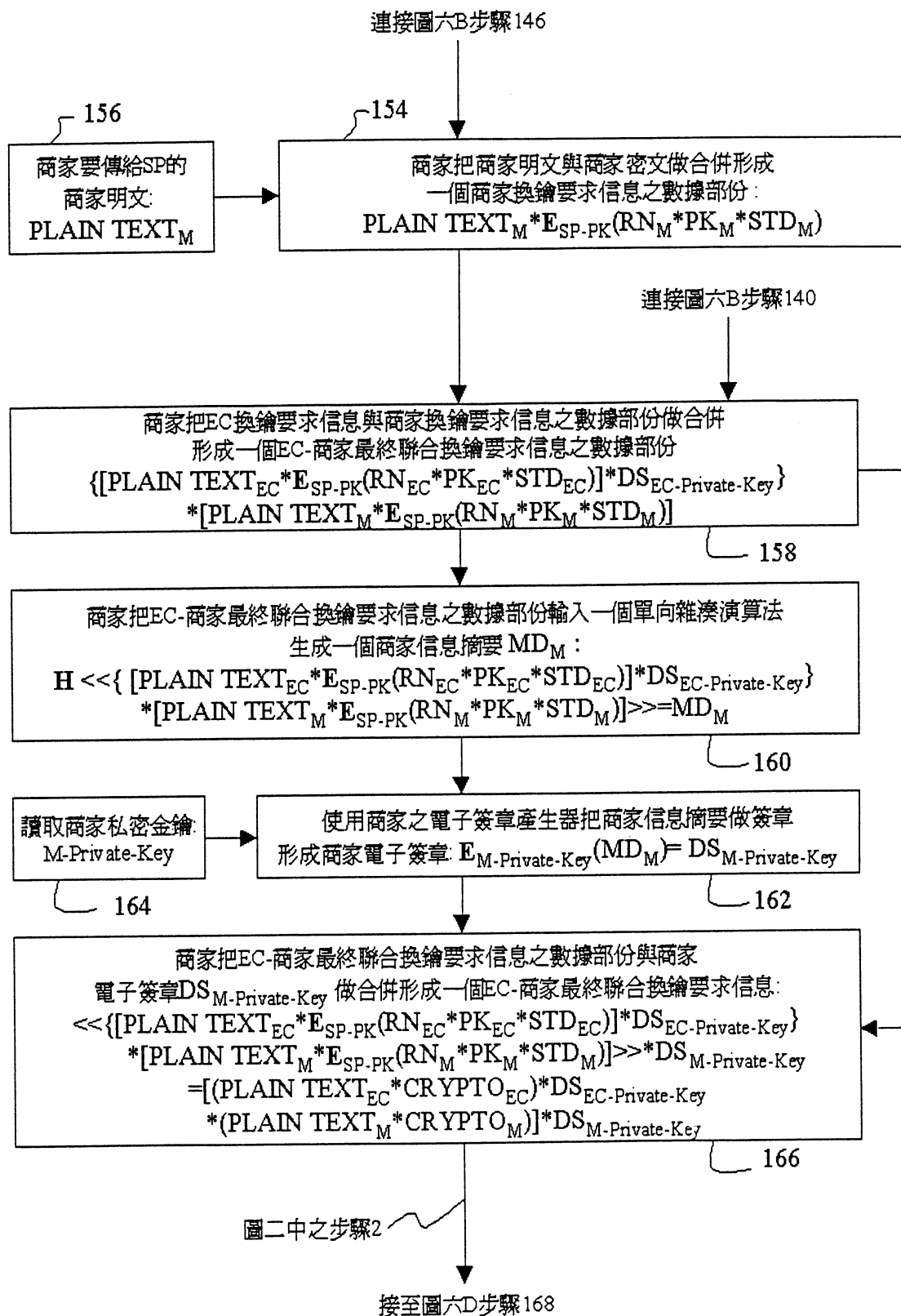
第 6A 圖



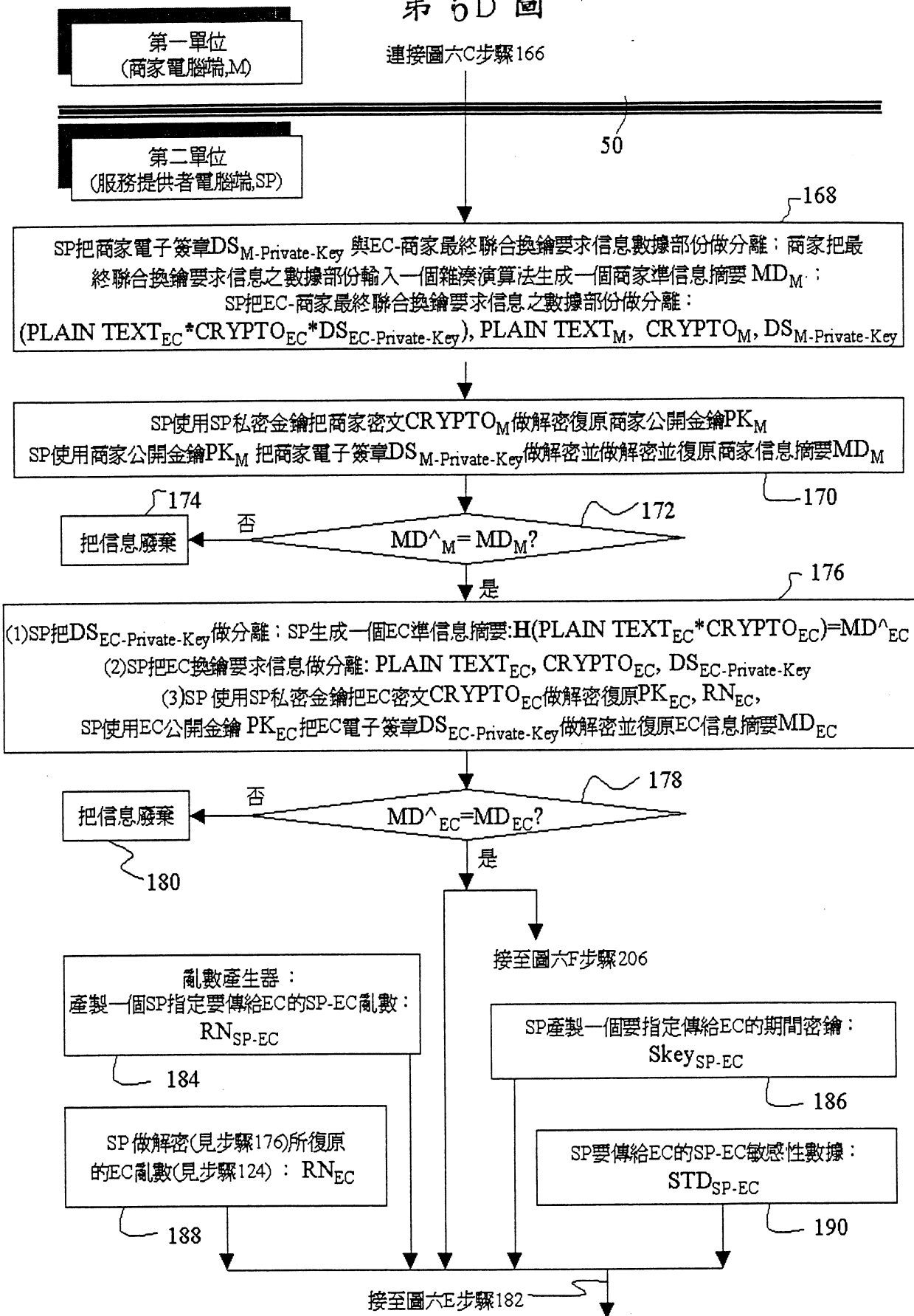
第 6 B 圖



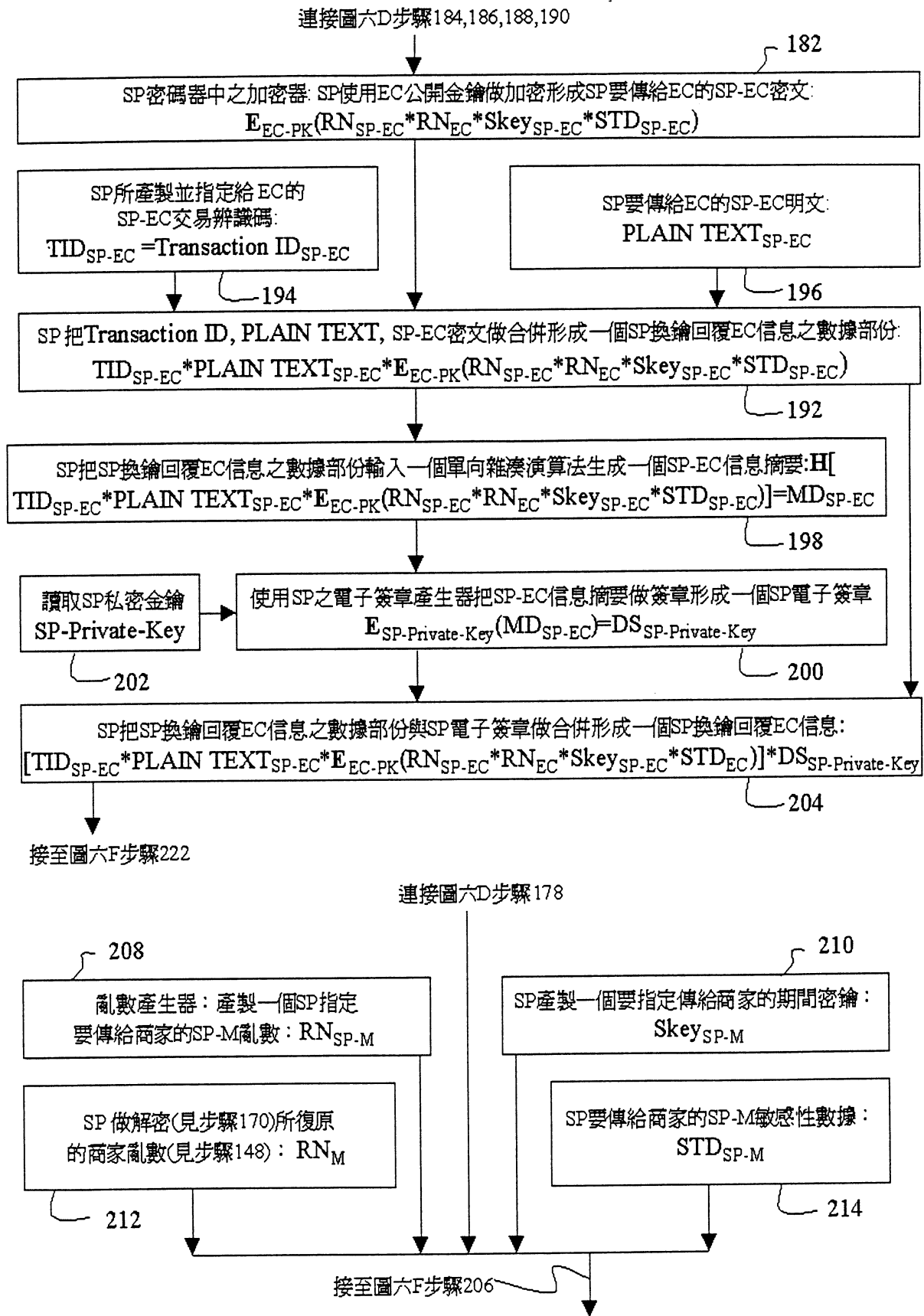
第 6 C 圖



第 6D 圖

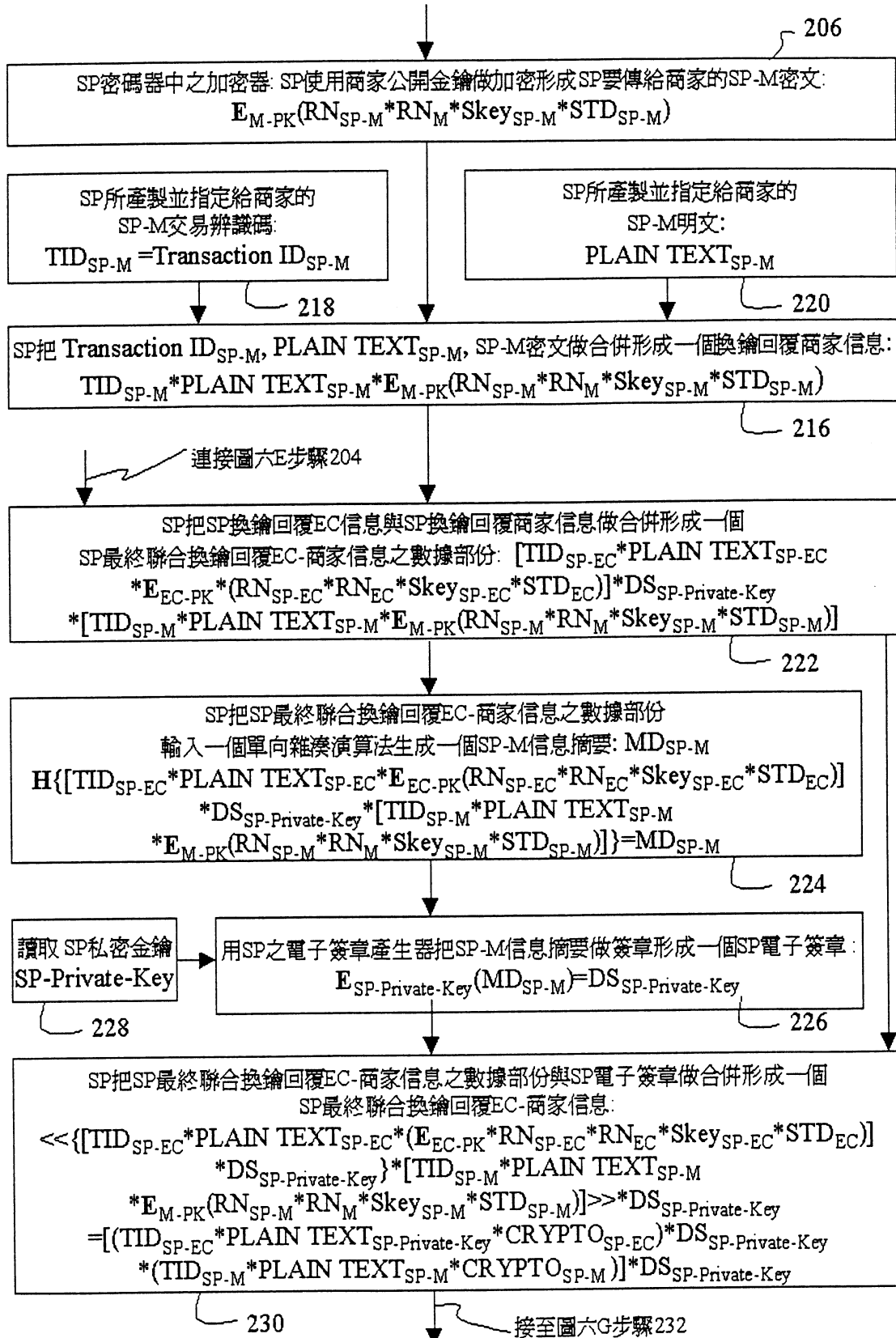


第 6 圖

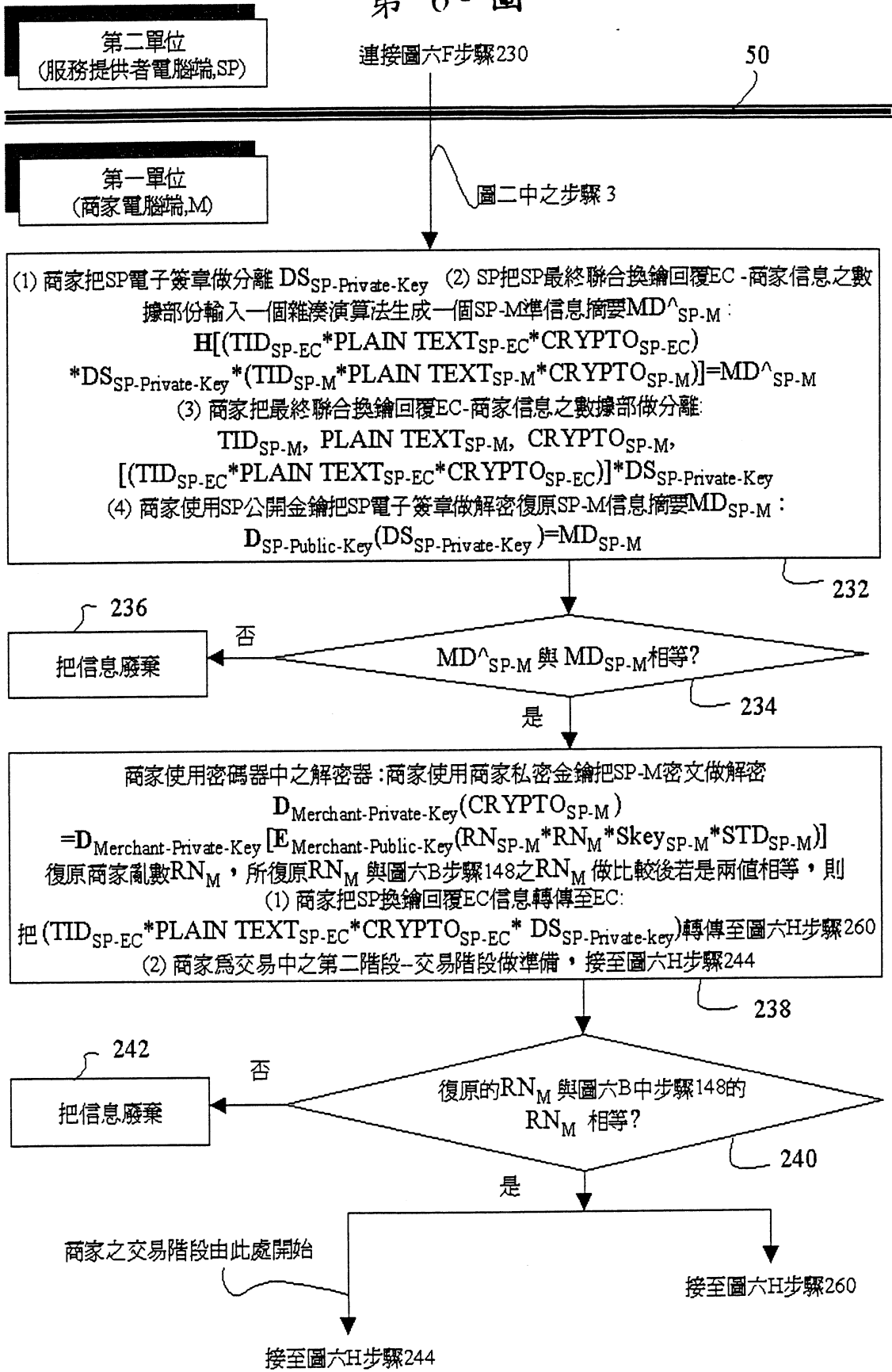


第 6F 圖

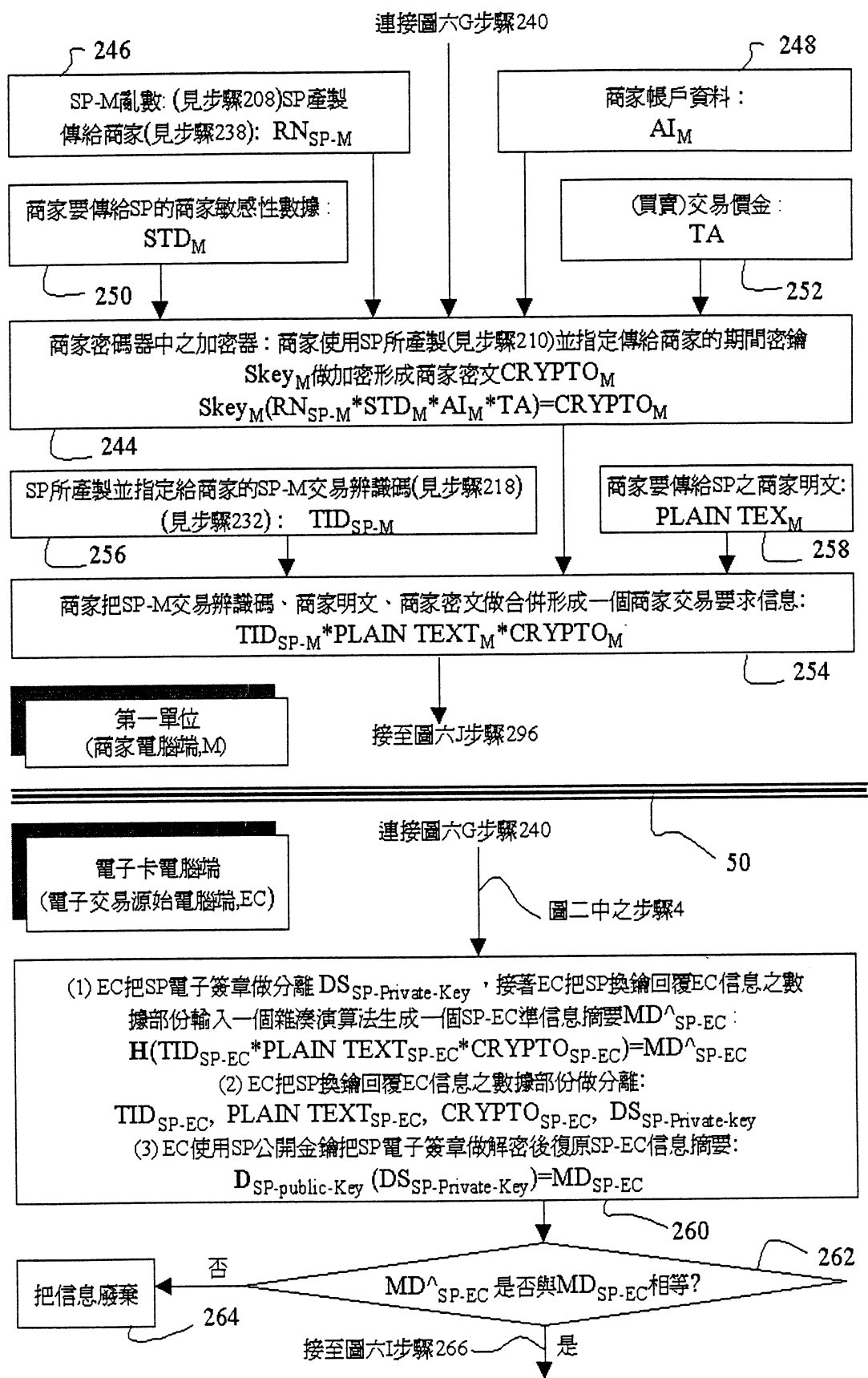
連接圖六E步驟208,210,212,214



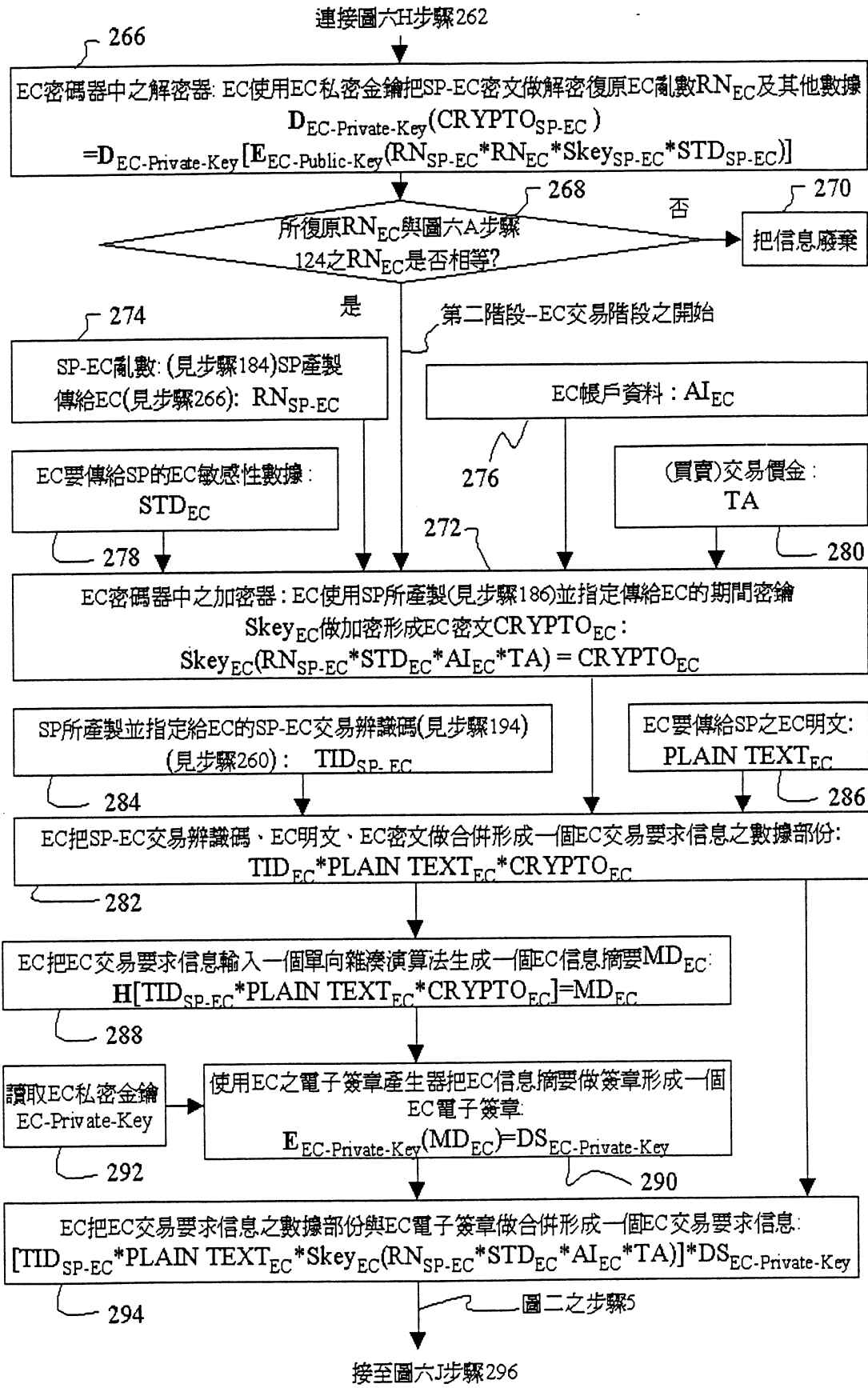
第 6G 圖



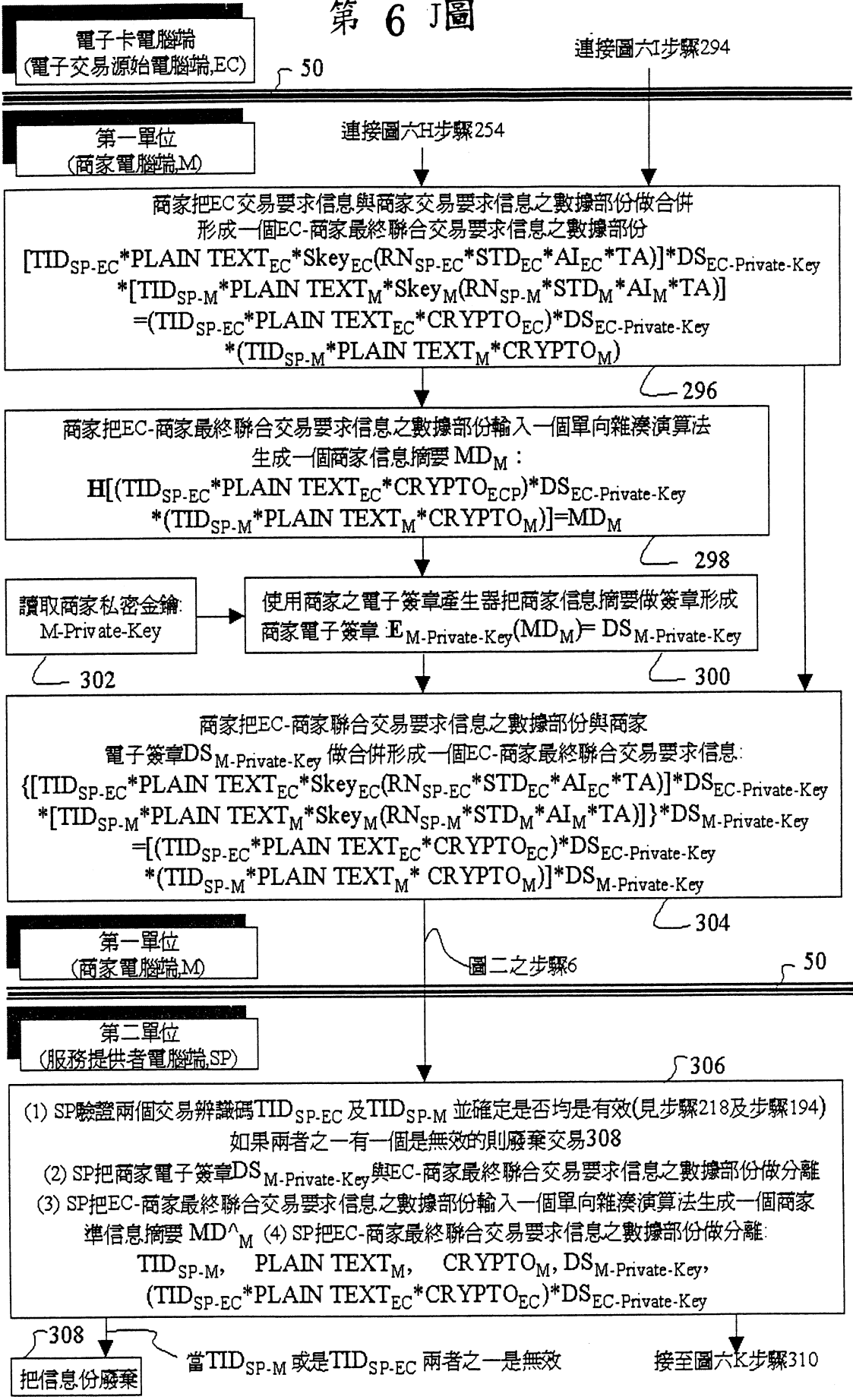
第 6 H 圖



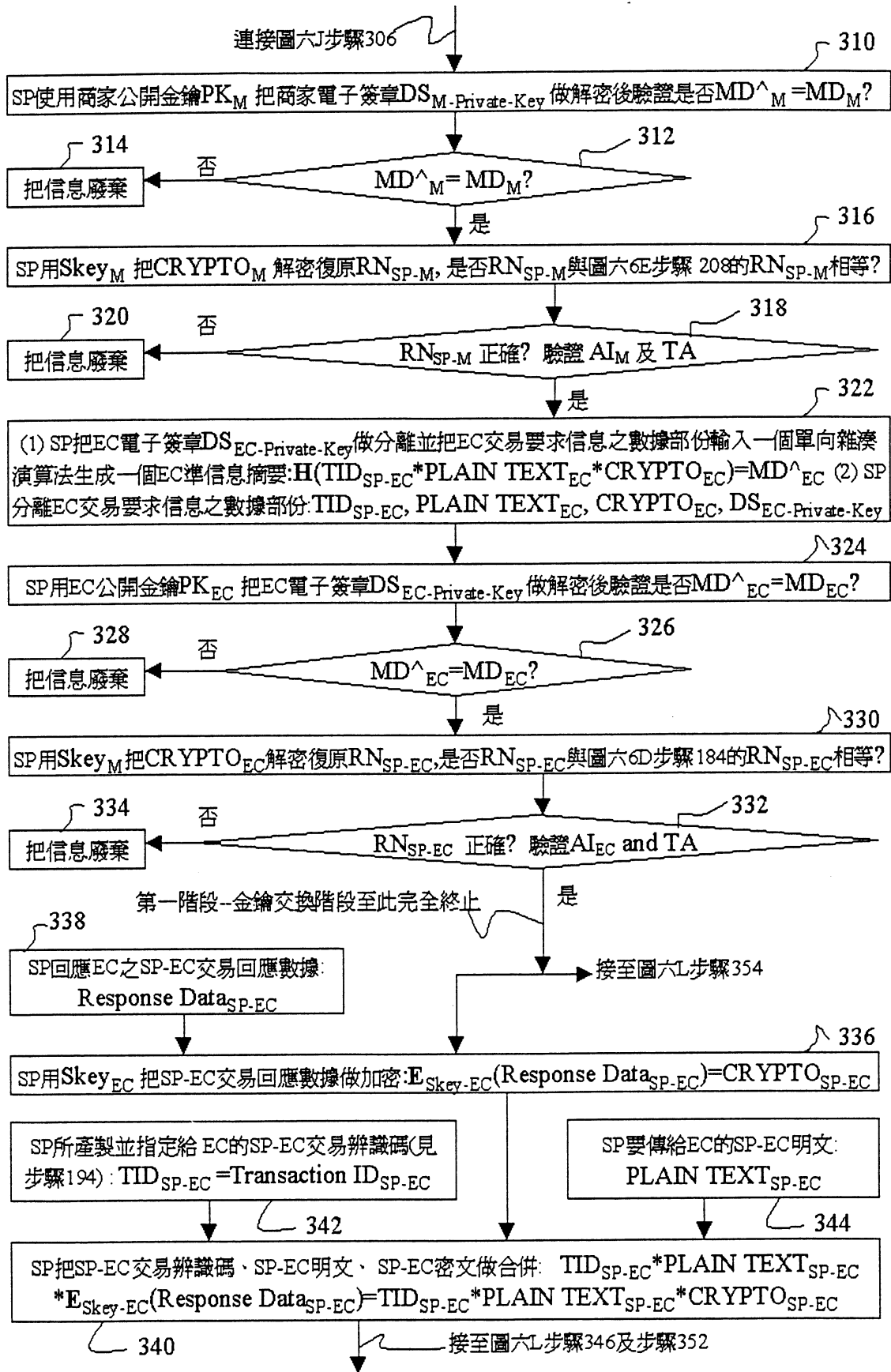
第 6 I 圖



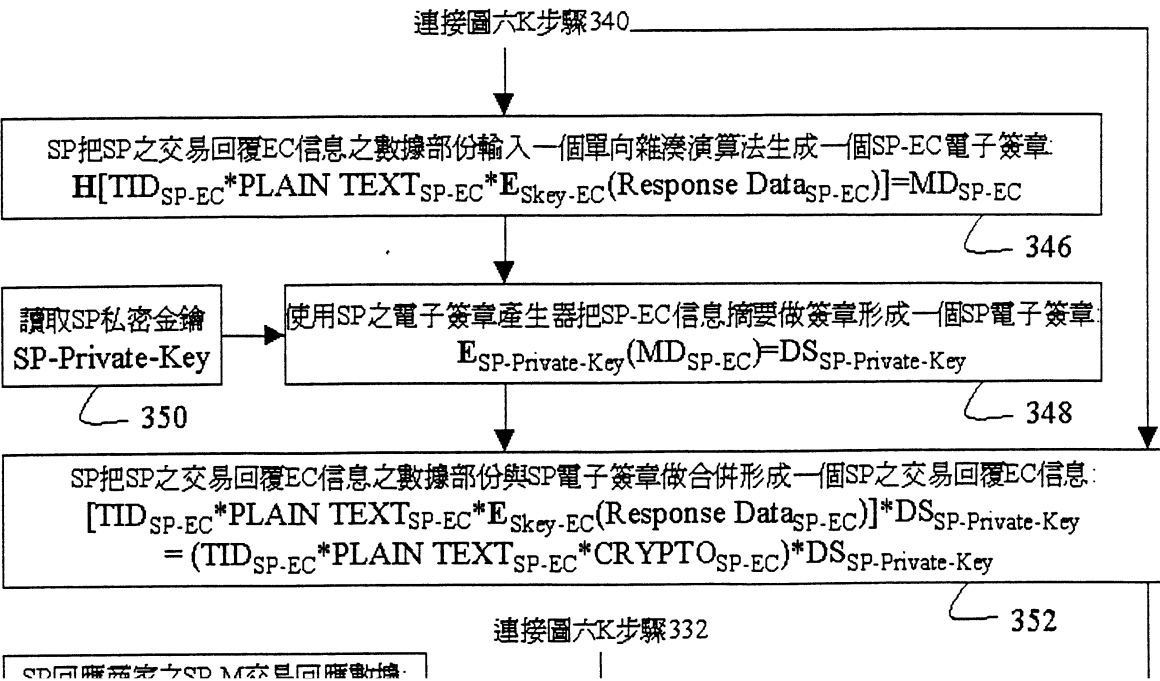
第 6 J 圖



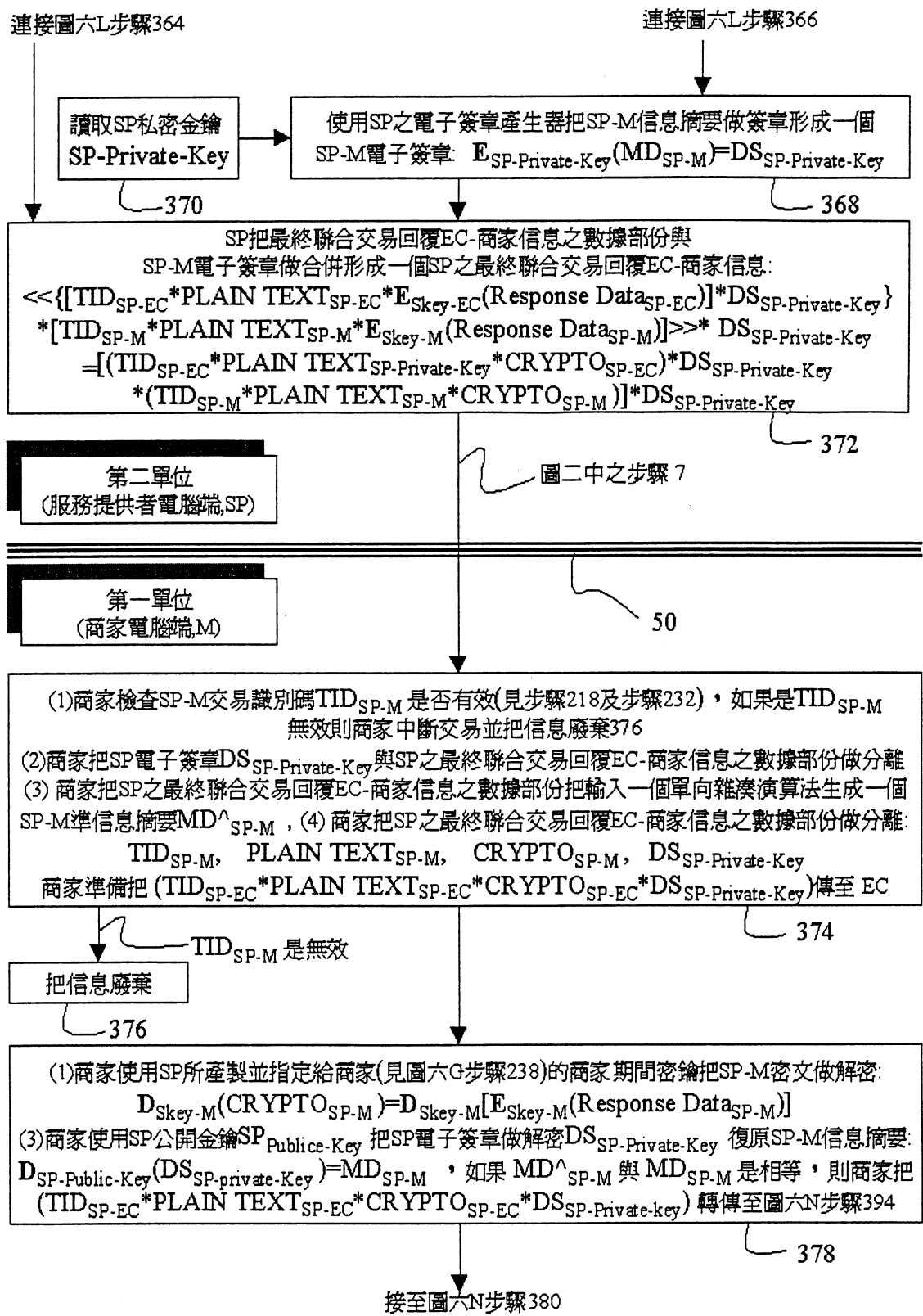
第 6 K 圖



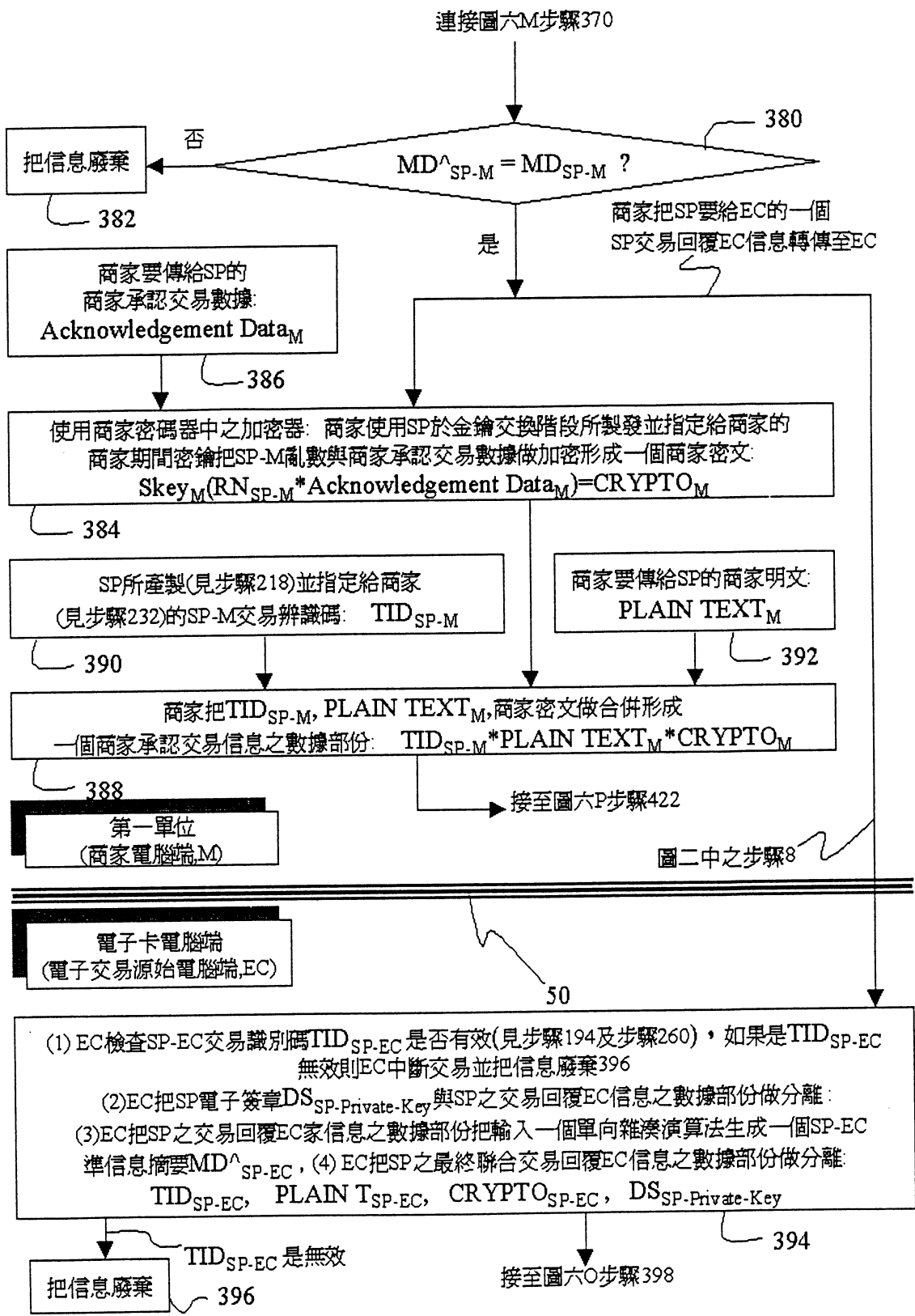
第 6 L 圖



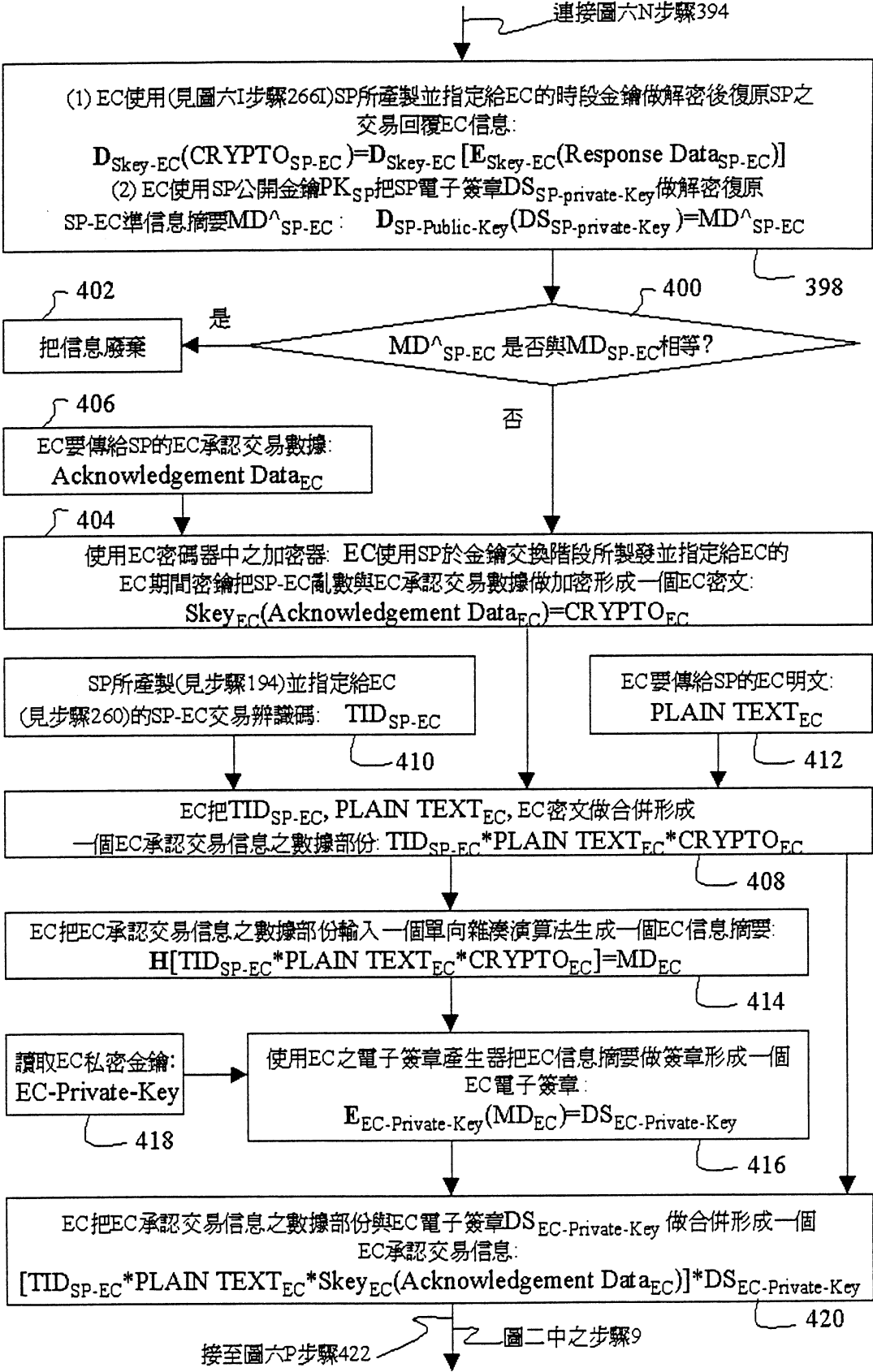
第 6 M 圖



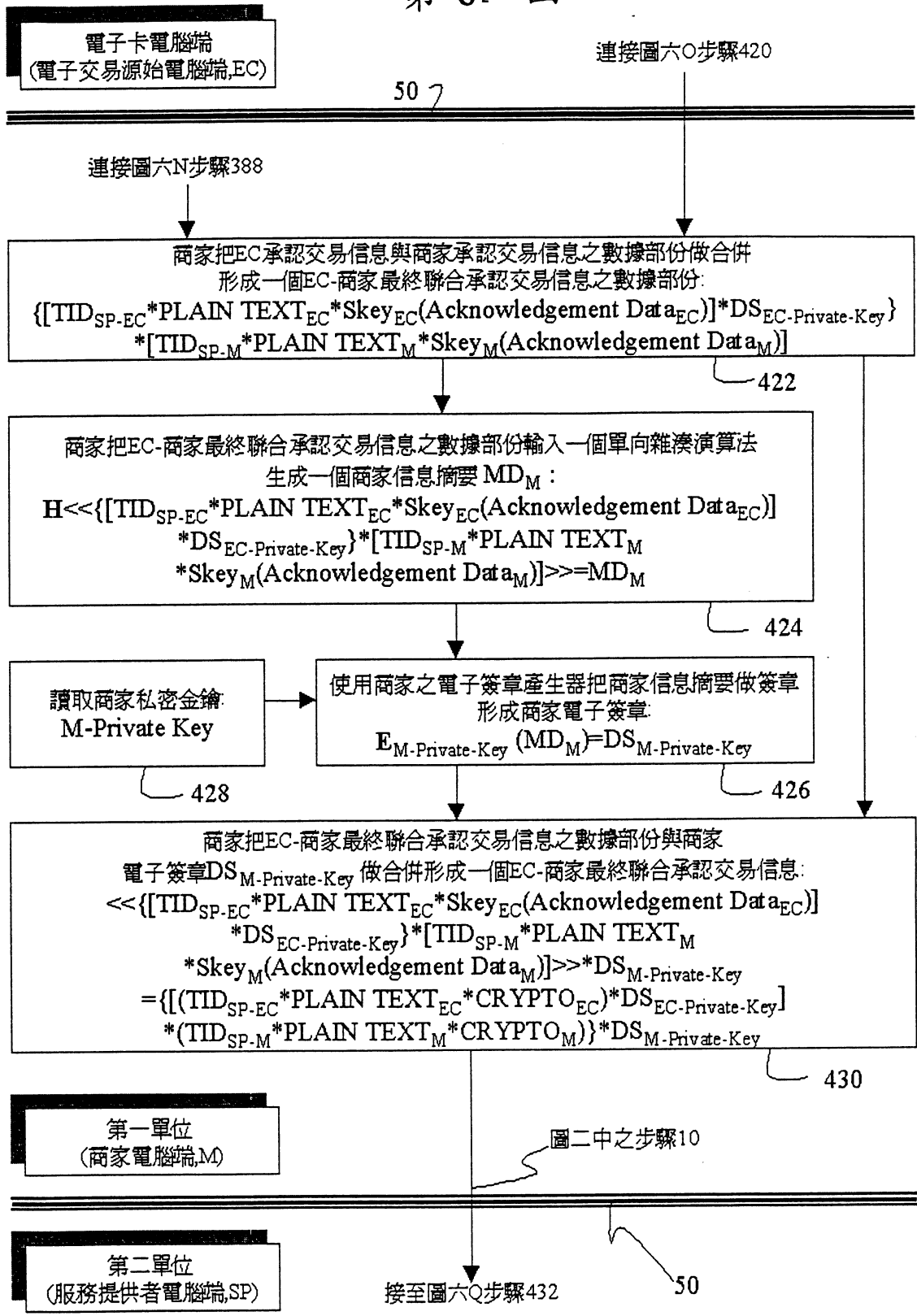
第 6 圖



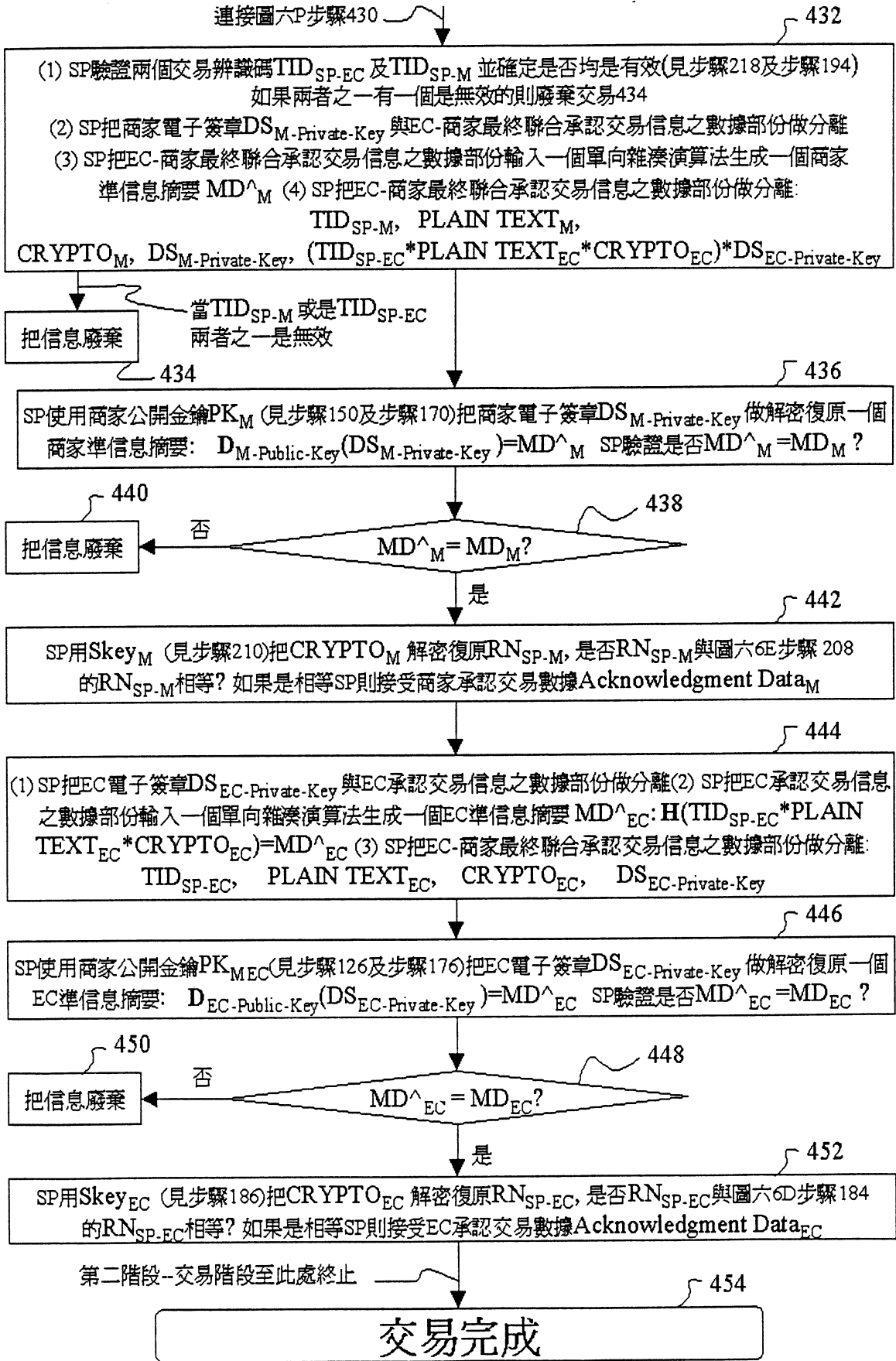
第 6 圖



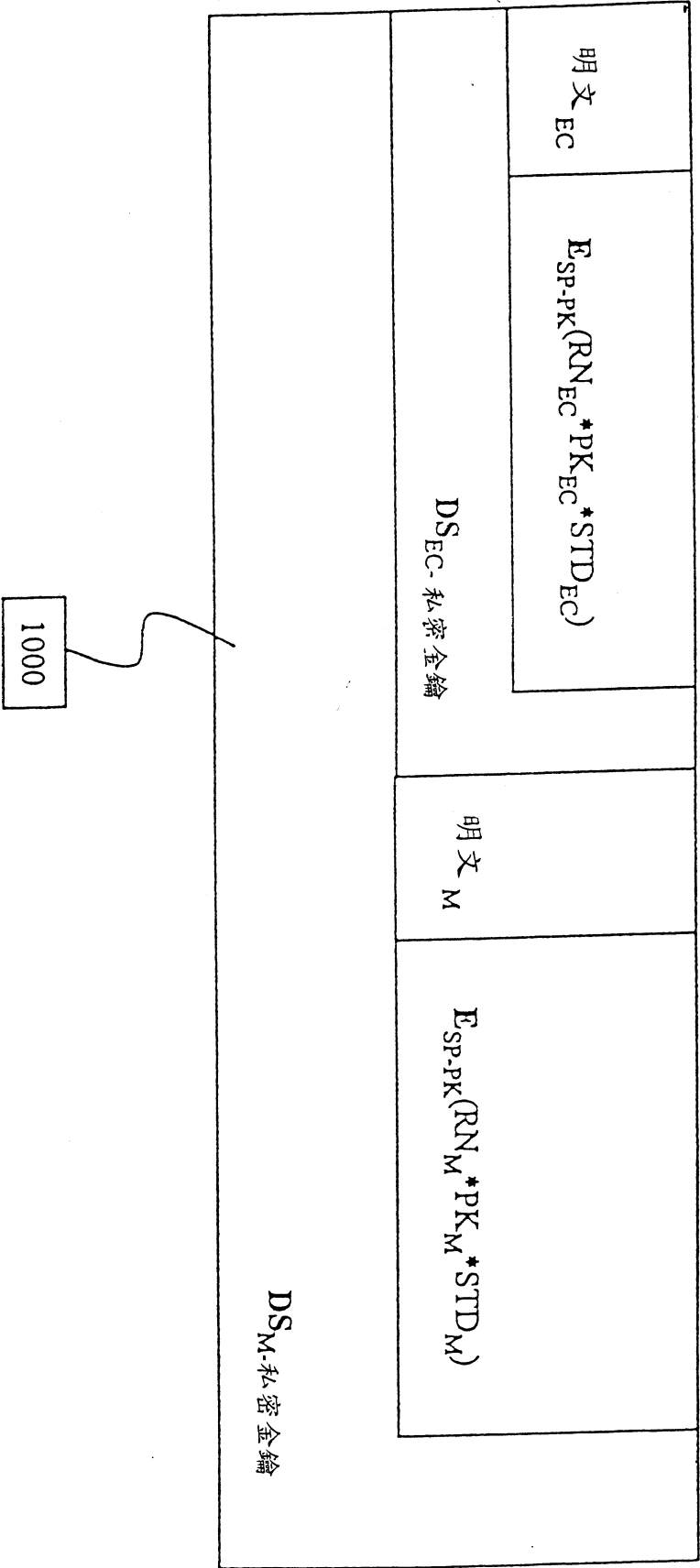
第 6P 圖



第 6 Q 圖

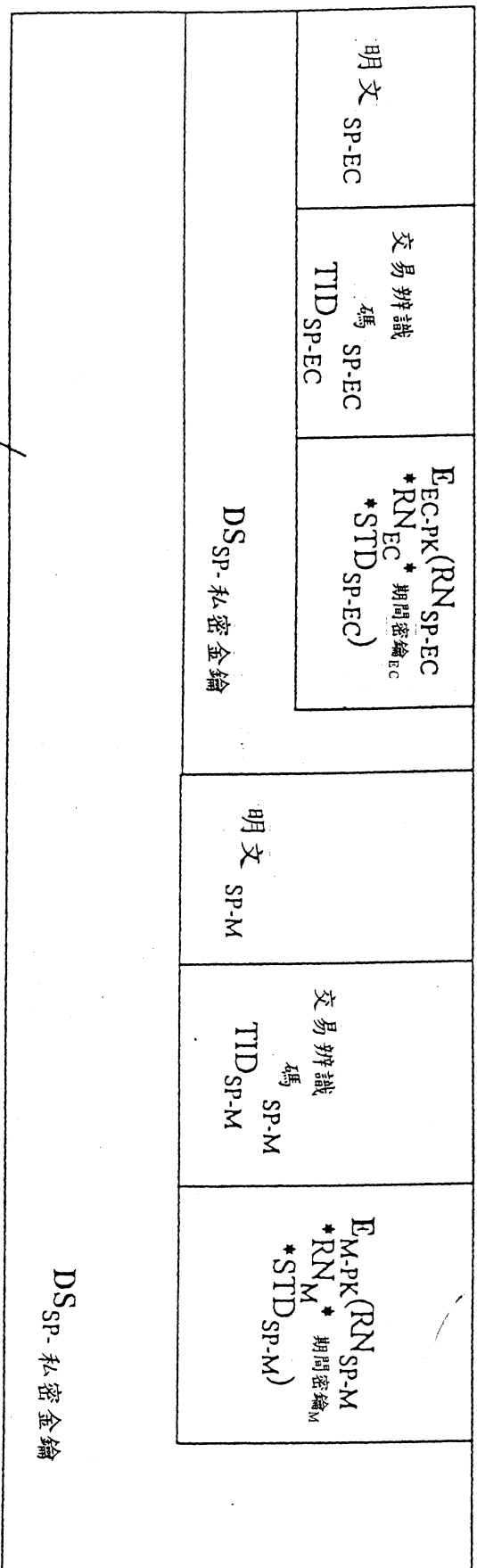


第 7 圖



煩請委員明示 90 年 7 月 13 日所提之修正本有無變更實質內容是否准予修正。

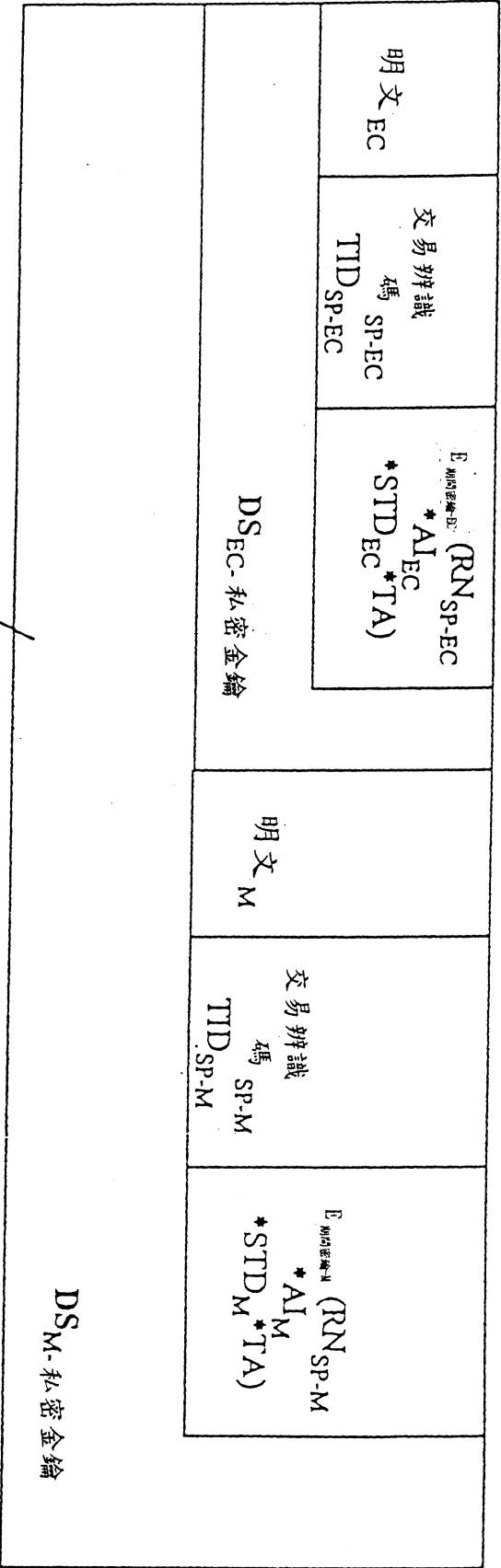
第 8 圖



1020

煩請委員明示
修正奉有
10年8月14日所提之
修正奉有
內容是否准予修正。

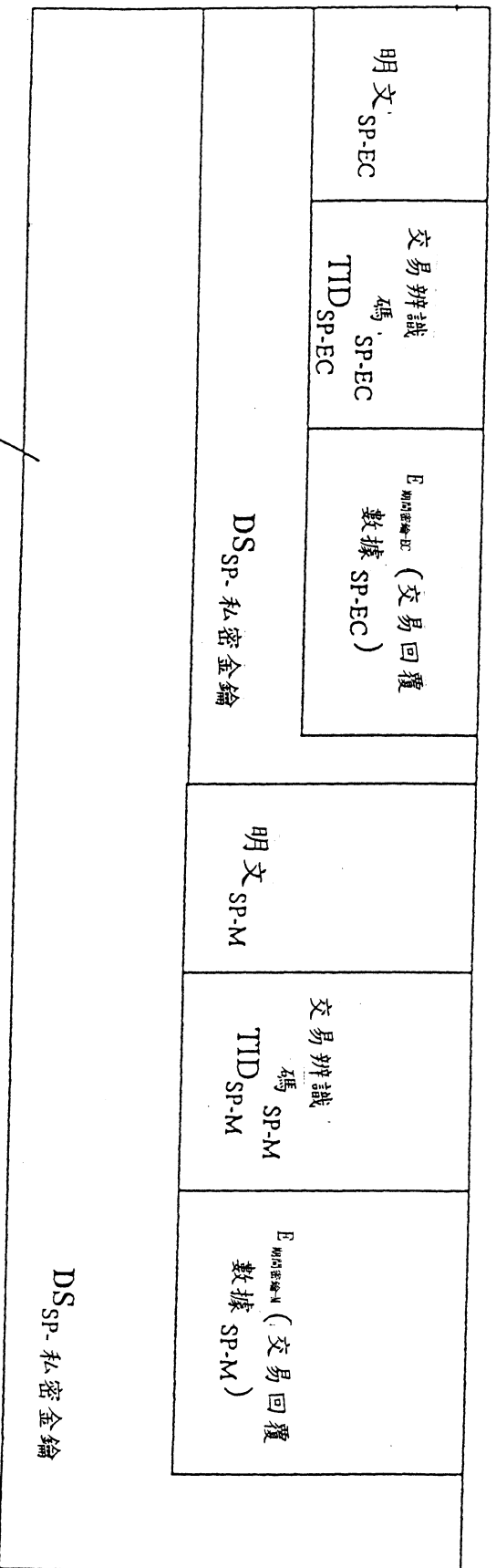
第 9 圖



正
補充

1040

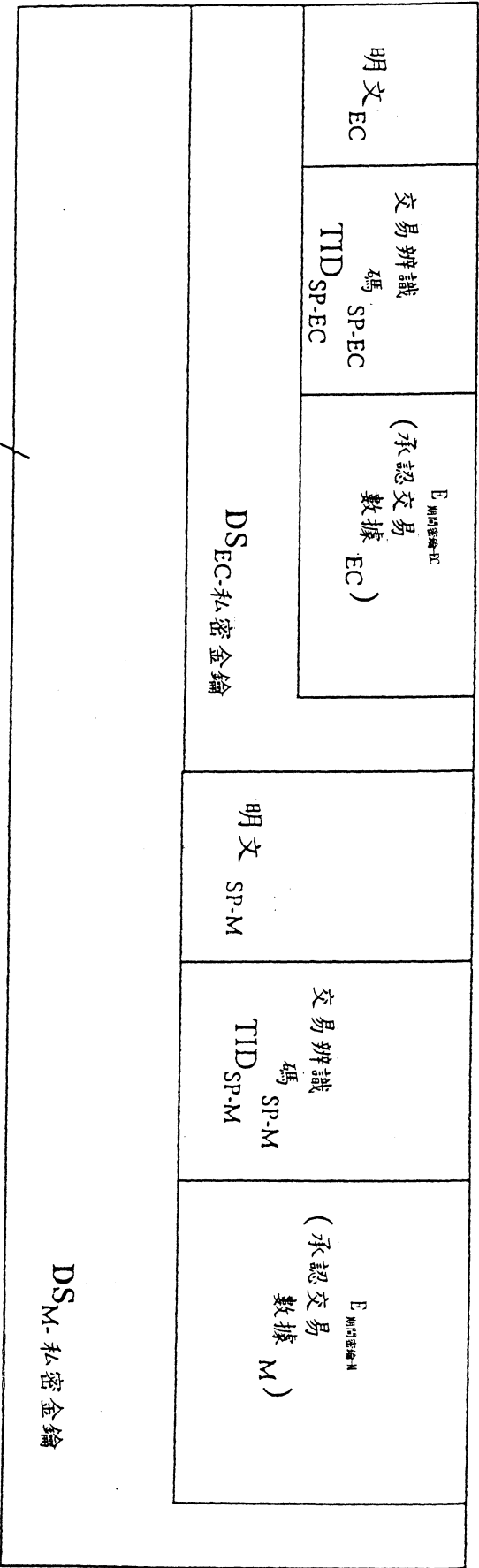
第 10 圖



1060

修正
補充
平成 8 月 14 日

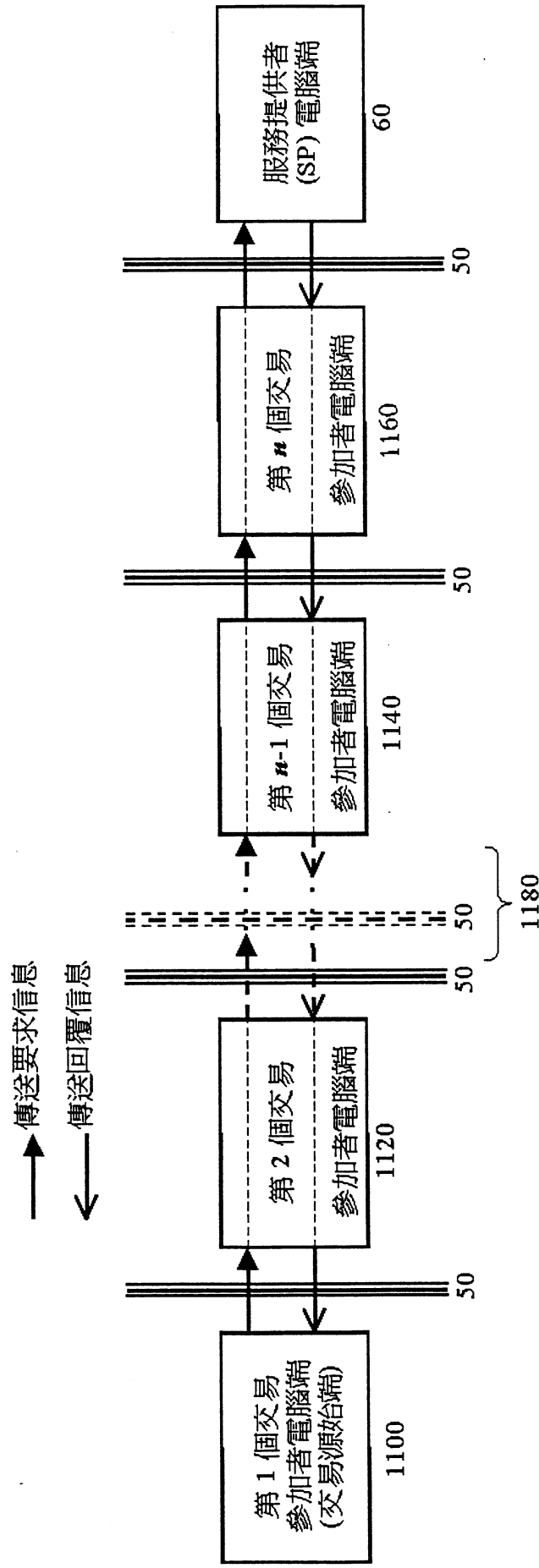
第 11 圖



1080

補充
R 年 8 月 14 日

第 12 圖



第 13 圖

