公告本

申請日期	94.6.13
案號	94120554
類別	G06F12/00

（以上各欄由本局填註）

A4
C4

484063

發明 專利說明書

一、發明名稱	中文	以不可分割方式修改特別是非接觸卡之晶片卡的非依電性記憶體的多個位置之方法
	英文	Method for modifying in a non-divisible manner a plurality of locations of the non-volatile memory of a chip card, in particulara contactless card
二、發明人	姓名	(1)法蘭柯伊斯・格雷憂 (2)史帝芬・狄戴爾
	國籍	法國
	住、居所	(1)法國巴黎市雷姆布利特路8號 (2)法國巴黎市米憂克路113號
三、申請人	姓名（名稱）	法商・英諾瓦特隆電子公司
	國籍	法國
	住、居所（事務所）	法國巴黎丹頓路1號
	代表人姓名	摩倫諾・羅蘭

裝 訂 線

經濟部中央標準局員工消費合作社印製

（由本局填寫）

承辦人代碼：	A6 B6
大　　類：	
ＩＰＣ分類：	

本案已向：

法　國（地區）　申請專利，申請日期：1998,4,9　案號：98 04453　，☑有　□無主張優先權

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）

本發明係關於微電路卡，特別係關於對本身之非依電性記憶體執行多種修改之微處理卡。

執行交易時，記憶體通常修改一次或多次，當然於利用新記錄資訊前必須確定全部修改皆正確，當有錯誤或記錄有訛誤時，新記錄的資訊必須被忽略或消除。

US-A-4 877 945敘述於複數資料項寫入過程中如何偵測異常以防交易基於錯誤情況持續下去。

於異常情況下，也希望可恢復原狀，換言之，隨後交易係對卡片執行不正確交易前已經記錄的資訊值進行。

前述US-A-4 877 945無法提供該優點，原因為某些案例中，當執行不正確交易時老舊資訊值已經喪失，故無法將資訊回復至稍早狀態，至少單純基於卡片所含資訊無法復原。

WO-A-89/02140敘述一種作業方式，但僅應用於單項資訊已被修改或複數項以彼此獨立方式修改的情況。

但許多案例中，於單一筆交易期間需要修改複數資料項，而此等複數資料項處理時須視為"彼此有交互關聯"，俾便確保複數資料項全部皆作妥善修改。

使用"無接觸"型卡片於此種情況下，卡片環繞終端機可正確作業的空間邊界無法察覺時，複數關聯資料項之交易不完美或不完全的風險特高。此種情況下，卡片與終端機間意外通訊中斷的風險無法忽略，可能由於卡片於處理結束前已經移離超過終端機的範圍，或因暫時性的干擾例如有一塊金屬通過旁邊。

五、發明說明（2）

一範例(當然為非限制性)為此種卡片用於遙控驗票交易，例如於大眾運輸網的入口，此時卡片扮演兩種角色：旅行車票；以及電子錢包角色。

曾經提出若干解決辦法來緩和前述困難且作複數寫入或其他修改至彼此相關的"無法劃分的"資料項。

前文舉例說明之特殊用途中已知系統始於由電子錢包扣帳，然後記錄使用者取得旅行權利。若使用者在兩次操作間抽出卡片，則要求使用者再度出示該卡片且重新開始寫入旅行權利。但若使用者走開而未再度出示卡片，則使用者可能出差錯。顯然無法以相反順序進行，後來使用者嘗試於錢包扣帳前抽取卡片係不可能。

該解決之道暗示終端機特別配置成於交易中斷的情況下激發例外處理來重新開始交易(要求將卡片重新插入終端機)。除了終端機的軟體特別複雜外，如所述該種解決之道並非全然滿意，若未重新開始交易使用者仍出差錯。

另一種解決之道在於資料交叉，終端機保留有關卡片的電子錢包狀態資訊，反之亦然。但該解決之道仍未臻滿意，原因為除了複雜以外也增加卡片與終端機間交換資料的容積，因而減慢交易的執行。當有多筆(三筆或三筆以上)寫入無法劃分時也難以應用。

本發明之一目的係提議一種致能以無法劃分方式於卡片記憶體作多次修改之方法。

本發明之另一目的係提出可完全由卡片執行之方法。如此可執行該方法而未修改終端機且無需於終端機提供另

五、發明說明（ 3 ）

外處理，該方法使用原有指令的語法，因此可選用的指令上極有彈性。

本發明方法屬於一型卡片於執行交易之時暫時耦合至終端機，交易包括終端機對卡片外加複數修改指令，各指令包含至少於卡片記憶體記錄由指令指定之個別資料項，藉此方式記錄的個別資料項彼此有交互關聯。以本發明之特徵方式，該方法包括由卡片執行下列步驟：a)當接收來自終端機之個別指令時，經由臨時將有交互關係之各項資訊記錄於卡片記憶體而臨時修改卡片記憶體但未喪失該項之對應先前數值；及然後b)經由全部確證或全部拋棄而結束修改，因此於隨後作業中，步驟a)執行的指令已經列入考慮，否則全部不受影響。

如此本發明原理包含將待進行的複數修改以無法分割方式集合於單一步驟a)，然後於修改已經執行後於卡片中整體確認此等修改。若確認成功，則其次由該卡片執行的操作(無論於相同交易期間或於隨後交易期間)，存取的內容必然反映出已經作的修改。

相反地，於步驟a)期間卡片進行操作有任何中斷則將取消全部執行的修改，非依電性記憶體中的資料保持於步驟a)之前的狀態。

特殊實務中，於步驟b)之確證情況下，於卡片記憶體記錄一旗標證實已經適當執行；當卡片隨後接收一指令要求步驟a)寫入之至少一資料項或其對應值被讀取及/或修改時，卡片開始檢視旗標狀態，若尚未記錄旗標，則卡片

五、發明說明（ 4 ）

忽略或取消先前於步驟a)所作的臨時記錄，並基於對應該資料項之先前數值執行該等指令。若卡片檢視旗標狀態時發現已經記錄，則卡片執行拷貝於步驟a)執行的臨時寫入作業。

最佳卡片適合以雙模作業，亦即對話進行中模，其中經由執行步驟a)及b)作記錄；及結束對話模，其中步驟a)及b)皆未確證作記錄。

開啟一段對話例如可以卡片復置為零表示或可於一指令具有兩種動作之後，一者執行預定作業而同時被解譯為開啟一段對話。

例如當藉一證明無法完成通常核准記錄時，卡片自動開啟一段於此對話進行中處理記錄。

以相同方式，結束對話例如可於一指令可執行兩種動作之後：執行預定作業且同時被解譯為關閉一段對話的指令。

例如電子錢包扣帳作業結束對話，因而避免須與所得的認可通訊，如此使對話認可與電子錢包交易認可變成無法分割。

更佳該方法包含認證功能組合結束步驟b)功能，於認證失敗的情況下強迫步驟b)被拋棄。

第一實務中，認證之執行方式係藉卡片進行其證實終端機的真實性及/或終端機與卡片間交換資料的真實性，卡片檢查由終端機產生加密認可並傳輸至卡片，唯有於認可被確認為正確時才證實於步驟b)的修改。

五、發明說明（ 5 ）

於對話模過程中可作臨時修改，故當卡片接收到來自終端機的指令要求修改記憶體內容且包括證實密碼認可時，證明該指令是否接收到結束對話，若指令係於對話進行中接收，則無需如此執行。

換言之，由卡片於步驟b)執行的指令以及通常(亦即結束對話)的指令證實加密認可，當係於對話進行中執行時，則不再含括此種確認，以"對話認可終端機的真實性"來執行相當的功能。

第二實務中，認證真實性係由終端機進行，其認證卡片的真實性及/或終端機與卡片間交換的資料之真實性，若且唯若於步驟b)確認修改，卡片以有條件方式產生並傳輸加密的認可至終端機。

於對話模中，可作臨時修改，故卡片接收來自終端機的指令用於修改記憶體內容且包括產生加密認可，若指令係於結束對話後接收，則進行該作業，若指令係於對話進行中接收，則無需進行該項作業。

換言之，由卡片於步驟b)執行的指令以及正常(亦即停止結束對話)產生加密認可的指令時，當係於對話進行中執行則不再產生此種認可，而以"執行認可證實終端機真實性"來執行相當的功能。

可作臨時修改，故當卡片於步驟b)接收到來自終端機的指令要求修改記憶體內容且包括產生複數加密認可時，該等認可儲存於步驟b)，且隨後共同傳輸至終端機，若且唯若修改已經於步驟b)獲得證實。

五、發明說明（6）

換言之，規定由卡片展期通訊通常由步驟b)之命令產生的加密認可。特別若核可的寫入指令產生某種寫入認可，則希望唯有於寫入已經不可變更的執行之後認可才離開卡片。

特定實務中，至少部分可能於步驟b)執行的指令包括選擇性抑制屬性，及若卡片於步驟b)於對話進行中執行此種指令，則該指令執行的修改係於步驟b)的結果獨立無關地執行。

換言之，該屬性定義指令係於對話進行中執行(亦即若對話未完成則將被取消)，或於結束對話時執行(亦即即刻有效仿佛已經完成對話，即使就時間上而言仍然處在對話進行中亦如此)。

最佳本發明於步驟b)之後且於確證修改情況下進一步提供下列步驟順序：d)終端機遵照卡片的確證執行某種動作；及e)若該動作由終端機妥適執行，則實證資訊記錄於卡片方便隨後藉讀取存取。

此種"實證"對話通知卡片於執行對話之後終端機確實可採行決策(例如應用於大眾運輸網的進出口開啟柵門)。

觀察到此種實證係由卡片處理而無需額外寫入(臨時寫入的拷貝則為遲早需要執行的作業)。此外，此種卡片於拷貝端執行的情況唯有當動作已經於終端機端適當執行的情況，換言之，唯有整個交易符合一致。

全部操作皆由卡片執行的情況下較佳規定步驟b)的記錄指令為內部指令，卡片於步驟b)之後接收到的任何指令

五、發明說明（7）

被解譯為命令記錄實證資訊於卡片。

其他特點及優點由後文說明本發明之二實施例顯然易明。

此等實例中且確實於全文中，"指定"一詞用以表示"特定複數中之一者"，且係有關於卡片所含的多個項目當中特徵化一項特定資訊的動作。

此種指定可能為內部者，由於指令本身規定一項特定資訊，例如指令"由電子錢包中扣帳x量"指示記憶體位在含有"電子錢包結餘"資料項數值。

指定也可為明確者，如下實例1所示，規定寫入指令有一位址或扇區識別記號，指令係藉指標i加索引。

實例I

提供一卡片其可儲存100個8-位元組值，且可執行下列命令：

*讀取於1至100範圍由指標i規定的8-位元組值v；

*寫入於1至100範圍由指標i規定的8-位元組值v；

*開啟一段對話；

*結束一段對話。

卡片在一次對話進行中至多允許三次寫入。習慣上使用大寫字母來標示非依電性記憶體(例如EEPROM)之值而小寫字母用於標示依電性記憶體(RAM，其內容當未供電時即消失)之值。

非依電性記憶體區段分配作業記憶體的主要資料儲存區(確定寫入)；

五、發明說明（ 8 ）

*V[i]對1至100範圍之i：100 x 8位元組。

另一非依電性記憶體區段分配給對話機制且包含：

*T[k]用於1至3之j：3 x 8位元組

含有一對話過程寫入之值(臨時寫入)；

*I[k]用於1至3範圍之j：3 x 1位元組

含有對話過程寫入值之指標；及

*C：於對話結束時寫入的計數位元組。

C編碼於對話過程中執行的寫入次數；適當冗餘機制(例如結合該值的補數)可偵測於計數位元組儲存值不確定的案例。

作業係如下進行。

步驟0：於卡片供電與執行第一指令間之瞬間檢驗C。若為1至3範圍之確定值，則對k等於1至C而言，於指標I[k]之值T[k]由表V[i]拷貝。隨後C復置至零及內部變數j設定為-1(指示尚未開啟對話)。

步驟1：讀取中，進行測試瞭解j是否大於0；若是，則要求的指標i對k由j至1以遞減順序與I[k]值比較。若有匹配則送返T[k]。所有其他案例則送返V[i]。

步驟2：於開啟一段對話時，j初始化為0(若對話已經開啟則取消)。

步驟3：於各次寫入時若j=-1(對話未開啟)，通訊值V係於T[0]寫入，通訊指稱i係於I[0]寫入，寫入C=0隨後v於V[i]寫入及寫入C=0；若0≦j<3(於對話進行中寫入)，則j遞增1，v於T[j]寫入，及i於I[j]寫入；若j=3則操作被拒絕

五、發明說明（ 9 ）

(已經超過一次對話進行中的寫入上限)。

步驟4：結束對話進行中，若j>0，則j於C寫入，然後對j為1至C，拷貝於表V[]於指稱I[j]之值T[j]。然後C設定為0及j設定為-1。

顯然卡片的電源可能於任一瞬間被中斷，讀取數值需正確，亦即對各指標i而言最末寫入值非於對話進行中，或寫入已經結束的對話(於一個非零值寫入C時，寫入已經完成或對話已經結束)。

增加加密以防當供給卡片的加密認可不正確時出現某種作業，及/或於某個作業結束時對卡片產生加密認可。

使用的加密認可係基於已知的密碼類型。例如"對話認可證實卡片的真實性"(或終端機)之獲得方式係當開啟對話時於卡片端及於終端機端對卡片(或終端機)供給的資料及/或對終端機(或卡片)供給的亂數應用安全雜散演算法(SHA)；由其中所得訊息確認碼(MAC)由卡片(或終端機)使用卡片(或終端機)所含密鑰藉數位簽章演算法(DSA)核章；終端機(或卡片)使用公鑰證實簽章。對稱加密演算法例如資料加密標準也可用於產生訊息確認碼(MAC)及/或產生簽章。

本發明中產生訊息確認碼之步驟為雙向認證所共通，且載於全部對話的資料。當使用對稱加密時，藉由認證卡片的認可及認證終端機的認可係由訊息確認碼編譯密碼之單一步驟獲得，卡片及終端機之認可係藉單元操作例如擷取某個預定位元導出。

五、發明說明（ 10 ）

實例II

本實例中，記憶體的資料被組織作為扇區，各個扇區包含四欄位：

1. 資料；

2. 識別者(可選定某個扇區之存取鑰)；

3. 合適性：若二節段具有相同識別者用於決定何扇區為適合；及

4. 檢驗：證實前三個欄位皆未訛誤(例如執行同位型檢驗)。

一扇區以其識別者標示，以此通知置換位置通知。扇區寫入過程具有一識別者作為參數隨同該識別者相關資料。讀取扇區程序有個識別者作為參數，其送返末次使用該識別者(或若識別者未曾使用則為適當指示)執行寫入時關聯該識別者的資料。換言之，係執行關聯型存取而非索引型存取。

讀取一扇區過程中，卡片搜尋扇區其帶有含要求值的識別者且非訛誤(藉檢驗欄位決定)。當多個扇區可滿足此兩項標準時，基於適合性欄位保有一特定扇區。

當寫入一扇區時，卡片將下列寫於適當扇區：要求的資料；識別者；適當欄位故於讀取過程中，此扇區為最適合的具有此種識別者之非訛誤扇區；及一檢驗欄位匹配前三欄位(換言之，寫入之處理方式為隨後可適當進行讀取)。

較佳寫入過程後，接著去除已經藉寫入新扇區而變成

五、發明說明（ 11 ）

不適合的扇區，如此可利用一新扇區。

較佳也提供(額外)資源回收型系統，亦即由一系統回收可能由於訛誤或由於不適合而已經無用的扇區。

較佳提供一系統其可延遲因寫入造成的磨耗，確保不會經常使用同一扇區，例如由可利用的多個扇區中隨機選用一扇區。

搜尋一扇區程序之概略優異變化方法包括利用搜尋步驟來消除已經發現訛誤的扇區及/或並非最適合的扇區，藉此重新產生自由扇區(於特定讀取過程耗費時間對隨後讀取與寫入速率有利)。較佳於消除一個已經發現為非訛誤但非適合的扇區前，再度寫入適合扇區原因為可能係寫入不當所致。

記憶體的工作量等於可利用的扇區數目減一個必須保持被消除的扇區。全部扇區(包括被消除扇區)係動態分布於記憶體內部。

若資料待於檔案結構化，例如應用ISO/IEC 7816-4標準結構化，則扇區識別者分成兩欄位：檔案識別者及檔案內部之扇區識別者。

使用此種特定扇區之結構之寫入/讀取作業之非限制性實務列舉如後：

後文說明使用此種特定扇區結構(非限制性)執行讀寫作業之說明：

*檢驗欄位以二元碼含有其他三欄位的零位元數目；顯然若有問題，例如中斷寫入或消除修改扇區內全部相同

五、發明說明（12）

方向的位元數目，則檢查檢驗欄位的數值可經常測知已經發生問題。

*適合欄位係以二位元編碼之0至3的整數。

*讀取程序循序讀取全部扇區至找到第一扇區具有尋找的識別者且非訛誤為止。若未找到任何扇區，則程序結束且報告"未找到扇區"。若找到第一扇區，其位置連同其資料及其適合性p儲存。持續搜尋。若找到第二扇區具有尋找的識別者且非訛誤，則測試其適合性q是否為p+1除以3整除的餘數；若是，則改寫第二扇區，消除第一扇區，及來自第二扇區的資料被送返；否則改寫第一扇區，第一扇區被消除，送返來自第一扇區之資料。若未找到第二扇區且若第一扇區的適合性為p=3，則此扇區被消除且報告"未找到扇區"；否則被送返的資料係來自找到的第一扇區。

*寫入程序類似前述讀取程序般開始。若找到先前儲存的扇區其已經由讀取程序藉特定識別者送返，則此扇區位置連同其適合性p(等於0、1或2)保留；若未找到此種扇區，則選擇一自由扇區(使用下述程序選擇)及識別者、資料、適合性p=3及檢驗欄位寫至該扇區，保留該扇區的位置及適合性。兩種情況下經由選擇一自由扇區(使用下述程序)繼續進行。識別者、資料、適合性p(計算為p+1除以3整除的餘數)，及檢驗欄位寫入此扇區。隨後若有任何先前儲存的扇區則消除之。

為了尋找一自由扇區，找到自由扇區數目n初始化於

五、發明說明（ 13 ）

零。循序檢驗扇區。對非空白且訛誤的扇區則消除之使其變空白(如此促成前述資源回收)；若扇區非訛誤及若適合性為p=3則消除之(也送到資源回收)；若該扇區非訛誤及若其適合性非p=3，則尚未掃描區段被搜尋是否有另一非訛誤扇區具有相同的識別者，若找到一者則非適合扇區被消除，如同讀取程序般進行；若此過程結束時扇區為空白，則找到自由扇區數目n遞增，隨機整數係以0至n-1之範圍取出；若整數為0，則儲存空白扇區位置。當全部扇區皆已經掃描時，全部非空白扇區皆非訛誤，並無任何兩個扇區具有相同的識別者，空白扇區數目n為已知，及其中一者已經儲存作為以相等機率方式的隨機選擇。若未找到自由扇區，則寫入過程中斷。

後文說明卡片使用此種特定扇區結構處理無法分割的修改對話之方式。

為了儲存無法分割的修改，卡片於非依電性記憶體有n個可利用的已經被消除的扇區(此處n對應於單一對話進行中可能需要作的無法分割的修改數目)。此外，卡片處理專用於處理一對話之非依電性記憶體區段(不含於扇區)，被稱作"對話描述者"。

此種實務並無對話之特定認證。

對話描述者係以三欄位定義：

*無法分割扇區的參考表單(LRSA)；

*形成無法分割扇區參考表單之檢驗值(VCC)；及

*考慮無法分割扇區參考表單之檢驗值(VCPC)，用於

五、發明說明（ 14 ）

發現對話是否結束。

步驟0：初始化：自從最近中斷卡片作業例如復置開始初次存取資料前，卡片必須確定對話描述者已經被消除。某些案例依據對話描述者的狀態需列入考慮。

*完全消除：卡片保持未改變；

*未完全消除，及VCPC為正確：卡片搜尋及消除(若有所需)全部已經被寫入而變化無用的扇區(來自參考表單)，然後消除對話描述者；

*未完全消除，VCPC被消除或不正確，及VCC完全正確：卡片消除LRSA所給扇區然後消除對話描述者；或

*未完全消除，VCPC被消除或不正確，及VCC被消除或不正確：卡片消除對話描述者。

步驟1：開啟對話：卡片尋找n個被消除的扇區，然後將參考表單記錄於對話描述者(假定被消除)之VCC。

步驟2：對話進行中：卡片接受指令。當其中一指令產生一或多個無法分割的修改時，用於記錄此等修改的扇區係記錄於LRSA至多高達全部n個修改扇區。

步驟3：結束對話：為了結束對話，卡片寫入VCPC，其確保LRSA及其VCC已經列入考慮。隨後搜尋並消除全部已經被寫入而變化無用的扇區(來自參考表單)。隨後消除對話描述者。

此外，若為處理實證的卡片，則對話處理包括下列修改：

步驟0：初始化：於對話描述者未完全消除及VCPC為

五、發明說明（ 15 ）

正確之情況下，卡片尋找並消除(若有所需)全部已經被寫入而變無用的扇區(來自參考表單)，但未消除對話描述者。

步驟1：開啟對話：卡片於依電性記憶體記錄對話被開啟。若對話描述者非空白，則卡片指示前一對話尚未被實證，經由分析LRSA甚至指示哪個資料項尚未被實證。總而言之未修改對話描述者。

步驟2：對話進行中：於第一指令帶有無法分割的修改時，若有所需卡片消除對話描述者，搜尋n個被消除的扇區，然後寫入LRSA及其VCC。

步驟3：結束對話：卡片於依電性記憶體記錄無開啟的對話。無論如何不消除對話描述者。

A5
B5

四、中文發明摘要（發明之名稱：以不可分割方式修改特別是非接觸卡之晶片卡的非依電性記憶體的多個位置之方法）

卡片於執行交易之時暫時耦合至終端機，包括終端機外加複數修改指令至卡片，各指令包含至少一記錄作業於卡片記憶體，指令規定的個別資訊項目，藉此方式寫入之各項資訊彼此有交互關係。該方法包含由卡片執行下列步驟：a)當接收來自終端機之個別指令時，經由臨時將有交互關係之各項資訊記錄於卡片記憶體，而臨時修改卡片記憶體但未喪失該項之對應先前數值；及然後b)經由全部確證或全部拋棄而結束修改，因此於隨後作業中，步驟a)執行的指令已經列入考慮，否則全部不受影響。

英文發明摘要（發明之名稱：Method for modifying in a non-divisible manner a plurality of locations of the non-volatile memory of a chip card, in particulara contactless card）

The card is coupled temporarily to a terminal while a transaction is being executed that includes the terminal applying a plurality of modification commands to the card, each comprising at least one operation of recording, in the memory of the card, a respective item of information specified by the command, the various items of information written in this way being mutually interdependent. The method comprises execution by the card of the following steps: a) on receiving corresponding respective commands from the terminal, it modifies the contents of the card memory by provisionally recording in the card memory each of said interdependent items of information without losing prior values corresponding to said items; and then b) the modifications are finalized either by all of them being confirmed or by all of them being discarded, such that for subsequent operations, the commands executed in step a) will either all have been taken into account, or else all of them will be without effect.

A8
B8
C8
D8

90.7.13 修正補充

六、申請專利範圍

第88105596號申請案申請專利範圍修正本　　90.7.13.

1. 一種修改微電路卡片之非依電性記憶體內容之方法，該方法中，卡片於執行交易時暫時耦合至一終端機，交易包括終端機對卡片外加複數修改指令，各自包含一記錄一在一記憶體之所給予扇區中的值之作業，藉此方式記錄的個別值係彼此互不相干，

該方法之特徵為包含卡片執行下列步驟：

a)當接收來自終端機的對應個別指令時，藉由臨時記錄數個該等在記憶體之個別扇區中之獨立值來修改卡片記憶體內容；及然後

b)結束修改，包括全部皆確認或全部皆被拋棄，而隨後作業，於步驟a)執行的指令全部皆列入考慮，否則全部皆無效。

2. 如申請專利範圍第1項之方法，其中：

*於步驟b)之確證情況下確證適當執行的旗標記錄於卡片記憶體；及

*當卡片隨後接收到指令要求於步驟a)寫入之至少一值被讀取及/或寫入，則卡片開始檢驗旗標狀態，若尚未記錄，則卡片忽略或取消先前於步驟a)所作的臨時記錄且基於被包含於步驟a)前之記憶中的對應值執行指令。

3. 如申請專利範圍第2項之方法，其中當卡片檢驗旗標狀態時，若旗標已經記錄，則卡片執行拷貝步驟a)所作臨時寫入的作業。

修正本有無超出原說明書或圖式所揭露的範圍 90 7 13

（請先閱讀背面之注意事項再填寫本頁）

訂

線

六、申請專利範圍

4. 如申請專利範圍第1項之方法，其中該卡片適合以雙模作業，亦即：

*對話進行中模，其中記錄係藉執行步驟a)及b)進行；及

*結束對話模，其中全部步驟a)及b)所作的記錄皆未獲得確認。

5. 如申請專利範圍第1項之方法，包含一認證功能結合結束化步驟b)之功能，於認證失敗時迫使步驟b)被拋棄。

6. 如申請專利範圍第5項之方法，其中該認證係由卡片執行，其認證終端機及/或終端機與卡片間互換的資料，卡片檢驗終端機產生並傳輸至卡片的加密認可，且唯有於認可被辨識為正確時才確認步驟b)的修改。

7. 如申請專利範圍第6項之方法，其中該卡片適合以雙模作業，亦即：

*對話進行中模，其中記錄係藉執行步驟a)及b)進行；及

*結束對話模，其中全部步驟a)及b)所作的記錄皆未獲得確認、以及其中當卡片接收到來自終端機的指令要求修改記憶體內容且包括加密認可證明；若指令係於結束對話後接收，則執行證明；若指令係於對話進行中接收，則未執行。

8. 如申請專利範圍第5項之方法，其中該認證係由終端機執行，其認證卡片及/或終端機與卡片間互換的資料，卡片係以有條件方式產生並傳輸加密認可至終端機，若

六、申請專利範圍

且唯若該修改已經於步驟b)獲得確認。

9. 如申請專利範圍第8項之方法，其中該卡片適合以雙模作業，亦即：

*對話進行中模，其中記錄係藉執行步驟a)及b)進行；及

*結束對話模，其中全部步驟a)及b)所作的記錄皆未獲得確認、以及其中當卡片接收到來自終端機的指令要求修改記憶體內容且包括加密認可證明；若指令係於結束對話後接收，則執行證明；若指令係於對話進行中接收，則未執行。

10. 如申請專利範圍第1項之方法，其中當卡片於步驟b)接收到來自終端機的指令要求修改記憶體內容且包括產生複數加密認可時，此等認可係儲存於步驟b)，然後共同傳輸至終端機，若且唯若該修改已經於步驟b)獲得確認。

11. 如申請專利範圍第4項之方法，其中至少部分可於步驟b)執行的指令包括選擇抑制屬性，及其中若卡片於步驟b)於對話進行中執行此種指令，則該指令執行的修改係與步驟b)的結果無關。

12. 如申請專利範圍第1項之方法，其中進一步規定於步驟b)之後且於修改已經確認後，執行下列步驟順序：

d)終端機執行卡片確認後的動作；及

e)若該動作由終端機妥適執行，實證資訊記錄於卡片上適合供隨後藉讀取存取。

六、申請專利範圍

13. 如申請專利範圍第12項之方法，其中該步驟e)之記錄指令為內部指令，任何於步驟b)之後卡片接收到的指令皆被解譯為命令記錄實證資料於卡片。