申請日期	84.8.31
案　　號	84113790
類　　別	G06F17/60

（以上各欄由本局填註）

A4
C4

577000

發明 新型 專利說明書

一、發明 新型 名稱	中　文	用於在通訊網路中執行安全交易之裝置
	英　文	Device for carrying out secure transactions in a communications network
二、發明 創作 人	姓　名	荷夫希倫(Herve HILLION)
	國　籍	法國
	住、居所	法國索倫斯-利斯-葛萊瑞斯 F-74570 卻茲布魯重
三、申請人	姓　名（名稱）	可瓦迪斯股份有限公司 Covadis SA
	國　籍	瑞士
	住、居所（事務所）	瑞士日內瓦普蘭-利斯-奎堤斯 CH-1228 珊堤奈爾龐特路 109 號
	代表人 姓　名	荷夫希倫 **Herve HILLION**

（由本局填寫）

承辦人代碼：	
大　　類：	
ＩＰＣ分類：	

A6
B6

本案已向：

歐洲國（地區）　申請專利，申請日期：　　案號：　　，□有　☑無主張優先權

2000 年 06 月 26 日申請案號第 EP00810556.1 號

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

本發明揭示一種可連接做為通訊網路終端機之裝置，用於在通訊網路中，尤其關於使用網際網路之例如電子商務(e-commerce)、電子銀行(e-banking)、電子稅務(e-tax)及電子郵寄(e-mail)的作業及在電傳通訊及限定存取系統(restricted access system)中執行保全交易。本發明尤其可應用在通訊網路之例如網際網路中的保全交易。其中加密資料使用諸如保全電子交易(Secure Electronic Transaction)(SET)之通訊協定(protocol)在發卡系統、商家地址應用(merchant site application)及銀行系統間通訊。本發明也揭示用於在通訊網路中執行保全交易之持卡人系統(cardholder system)，包含裝置連帶局部電腦應用(local computer application)(LCA)，裝置連接到諸如個人電腦(PC)。

技術背景

在未保全通訊網路之例如網際網路中執行保全交易已有許多建議。

例如，通道保全(channel security)方法之諸如保全HTTP(S-HTTP)及保全插口層(secure socket layer)(SSL)通訊協定，用來在兩個通訊者之間產生保密(confidence)。S-HTTP使用具有嚴密加密鍵之數位簽名訊息(digitally signed message)來保證保全性及真實性(authentication)。SSL使用數位簽名證明(digitally signed certificate)嚴密地以加密訊息來提供真實性及保

五、發明說明（2）

全性。通道保全技術產生保密傳送資訊，但沒有保護在交易中商家及銀行來防止所涉及交易之"真僞"卡號，也沒有保護客戶來防止其個人資料之妄用，而且不讓銀行保證付款給商家。

多數群體通訊協定也被建議用於信用交易(credit transaction)，諸如保全輸送技術(STT)、網際網路鍵入付款(ikp)及保全電子付款通訊協定(SEPP)。上述 SET 保全付款技術代表在根據網際網路付款過程中之最新技術。最近，根據 SET 通訊協定所稱爲 EMV 之新規定(Specification)已由 Euro Card-Mastercard-Visa 開發計劃未來實施。

SET 通訊協定是由證明授權單位(certificate authorities)根據 SET 證明之管理及驗證的信託層系(hierarchy of trust)來設計，顯然地是在持卡人證明授權單位(其發行信用卡給持卡人)、商家證明授權單位(其發行證明給商家)及付款管道(payment gateway)證明授權單位之間，控制 SET 付款管道。SET 通訊協定是根據數位化證明之交換來提供銀行保證。SET 防止付款卡之詐欺使用，及防止第三者截取保密之資訊。

該通訊協定在銀行及商家之間提供良好保全性，但是如上述通道保全方法，對個人使用者沒有提供完全保全性。例如當使用者經過網際網路所連接 PC 來輸入資訊時，雖然如 PAN 或 PIN 碼之使用者私人資料以加密形式經網際網路傳送，使得加密資料僅能以受授權單位來解

五、發明說明（ 3 ）

密，但是未編碼資料曝露在未受授權者之"攻擊（attack）"。如此導致妄用及相當大量關於未授權交易之訴訟（litigation）。

讀卡機（card reader）用於接受所謂智慧卡（也稱為晶片卡、IC卡或ICC，以下統稱為ICC或簡稱"卡"）也是眾所週知。讀卡機通常包含：按鍵（keypad）、用於在保全交易進行中顯示相關訊息之顯示器（display）、微處理器（microprocessor）及記憶體（memory）。然而，習用讀卡機沒有克服上述問題，而通常各型讀卡機具有特定用於特殊應用之限制。

發明概述

本發明之目的在於提供一種可連接到諸如網際網路之通訊網路其做為終端機的裝置，用於經過網路來執行保全交易，提供使用者之完全保全性（fullsecurity），而且其可配合不同應用來使用於許多不相同之保全交易，例如，關於e-commerce（電子商務）、e-banking（電子銀行）、e-tax（電子稅務）、e-mail（電子郵寄）、電傳通訊及限制存取系統之作業，使得其非常多樣化。

本發明提供一種可連接做為通訊網路終端機之裝置，用於在通訊網路中執行保全交易，該裝置包含：按鍵、用於顯示在過程中有關保全交易之訊息的顯示器、微處理器、較佳地DSP微處理器及記憶體，包含非揮發性記憶體及RAM（隨機存取記憶體）。

裝置之非揮發性記憶體（下文範例如E^2 PROM）配置來

五、發明說明（4）

儲存三個層殼（shell）之軟體（software），啓動層殼（boot shell）、系統層殼及應用層殼，其中啓動層殼包含非可載入基礎軟體，其管啓動作業（boot operation）及軟體載入系統層殼及應用層殼。

裝置連同可載入或已載入非揮發性記憶體內之軟體，即系統層殼軟體包含作業系統軟體，其管理應用層殼、ASN資料庫（library）及加密／解密工具盒（tool box）及視需要之卡管理器（card manager）；而應用層殼軟體包含管理用於保全交易應用之軟體。

可載入應用層殼軟體包含一種應用，其當軟體載入非發性記憶體而裝置連接到通訊網路時，在使用者經按鍵鍵入編碼來執行保全交易時，配置來實施裝置之內部編碼加密作業。例如，編碼可以是PAN或PIN碼，其輸入構成交易接受之必需步驟。該應用在軟體載入非揮發性記憶體而裝置連接到通訊網路時，配置使得經按鍵所輸入編碼在裝置內加密，而輸出加密編碼，而所載入編碼不能自裝置外部來存取。

例如，當編碼鍵入時，未加密編碼瞬間先儲存在RAM之不能讀取部份，不可自網路存取。瞬間所儲存之鍵入編碼加密（整個加密通常以所載入加密工具盒來執行），然後在加密後即自RAM來刪除。然後，所加密編碼自裝置內來輸出到通訊網路，例如，響應輸入接受編碼之使用者。如此使得以使用者鍵入PAN及／或PIN或PIN編碼能接受保全交易，而沒有未加密PAN及／或PIN編碼可自

五、發明說明（ 5 ）

通訊網路來存取。

而且，該裝置使用簡單，而重要地可以DSP技術以低成本來製造，使得其可使用該裝置用於鉅額及小額付款及大範圍之保全交易。

根據本發明之裝置是一種可驗證鎖(veritable lock)允許保全核對密碼(secret code)(例如，PAN編碼連同磁卡或智慧卡、或PIN編碼連同智慧卡)，而沒有任何未加密密碼傳送到通訊網路，即經個人電腦之CPU連接到網際網路及所連接裝置。

至少部份加密在裝置內實施：加密簽名在裝置內產生，而且PAN及／或PIN在裝置內加密。當在網路上之交易受到諸如SET之通訊協定保護時，交易也能以裝置來簽名。SET發行者能證實裝置真實性，而且發行者具有在保全標準之保險。其可能然而不需在裝置內側來管理SET證明。

裝置內可具有大量可用記憶體(例如8Mbit)，所以可以安裝許多應用。

裝置的主要優點之一是因為所使用DSP處理器的交易速度。該性能以處理用於資料加密或解密之大量計算來允許所傳送自或到網路(通常經所連接之PC)之資料的高程度保護。例如，裝置使用具有完全小於5全幕次之1024位元的RSA公用鍵(public key)能使得資料加密。

裝置連接ICC使用在通訊網路上實於保全交易，優點在，裝置使得在線上卡(on-line card)真實性能證實。為

五、發明說明（6）

此目的，裝置較佳地包含用於ICC卡之讀卡機，配置使得裝置在隨後所插入讀卡機內之ICC能卡識別及接受卡，如果以上述作業卡被接受則建立交易接受。至少一部份該卡識別及接受作業及／或該交易接受作業可具有優點地作用在裝置內插入之ICC所併合的處理器來實施，如下文將更詳細說明。

在本文中，商家驗證因而根據本發明之裝置在封閉保全環境中作業，其中該裝置以電子簽名來提供購買者之真實性確定。交易之在線上授權提供付款或其他交易之保證。卡簽名控制在線上(on line)進行，而不是離線(off line)。沒有可能詐欺，因此持卡人沒有不付款、沒有訴訟及扣回款要處理。

裝置之重要特徵是其能力在於載入系統及應用軟體，及使用所載入軟體用於實施包含以通訊網路建立保全交易的作業。尤其在銀行業，經常有變更致使軟體很快變得過時。裝置之載入能力使得根據軟體發展而能一直更新，尤其更新或升級應用可自伺服器或自可連接到通訊網路之局部電腦軟體來載入裝置內。

爲了允許軟體升級，裝置之非揮發性記憶體(E^2PROM)可包含緩衝區做爲緩衝記憶體，在載入作業期間用於暫儲先前載入系統及／或應用軟體，記憶體連同裝置來響應表示載入作業中斷或失敗之信號，用於重新載入在緩衝記憶體內所儲存之系統及／或應用軟體。

根據本發明之裝置可併用各種裝備，其一特殊實施例

五、發明說明（ 7 ）

是外部讀卡機可較佳地經USB連接器來連接到個人電腦。此讀卡機可包括在使用中可手持或安置在支架面上之以人體工學所設計讀卡機本體，本體具有用於容納ICC之槽，使得在使用中一部份ICC突出而當作業完成時來提醒卡移除。讀卡機本體也整合按鍵(keypad)及顯示器，且內部容納記憶體。

另一實施例是個人電腦之分離鍵盤(keyboard)併用根據本發明之裝置，鍵盤經USB連接器可連接到個人電腦。鍵盤之主按鍵組也可使用做為裝置按鍵，或裝置可具有沿著鍵盤之一所安置的專用按鍵般鍵側。鍵盤可併用其自己用於有關保全交易之訊息的顯示器，或電腦顯示屏幕可使用於顯示。較佳地其也具有用於容納ICC之槽，因而鍵盤也使用做為讀卡機。

根據本發明之裝置也可併用於可攜式個人電腦，本情形中，裝置必需具有其自己之記憶體及按鍵和電腦硬體分離而可對通訊網路來存取。然而，PC's之顯示幕也可使用做為裝置之顯示器。

進一步實例是數位電視接收機之視訊轉換盒(set top box)可經拋物線天線、行動通訊裝置之諸如經衛星之蜂巢式系統可連接到通訊網路的電話、固定式電話機及銷售點販賣裝置之諸如用於租用影像片匣的經銷商來連接到通訊網路，其全都可併用根據本發明之裝置。

本發明也揭示用於在通訊網路中執行保全交易之持卡人系統，包含裝置如上述連同局部電腦之諸如較佳地以

五、發明說明（ 8 ）

USB 連接器來連接到裝置的 PC。此一持卡人系統中，局局電腦可儲存軟體，包含動態鏈接資料庫(dynamic link Library(DLL)用於配合載入在裝置之非揮發性記憶體之系統殼層軟體及應用殼層軟體來執行網路中之保全交易。

本發明之另一架構是一種通訊網路，其中加密資料如上述在發卡系統、商家地址應用、付款管道及裝置或持卡人系統間來交換，其中裝置連接到通訊網路來形成在網路中用於執行保全交易之終端機(terminal)。尤其其中發卡系統、商家地址應用及付款管道根據 SET 之通訊協定來交換電子證書的交易。裝置以結合根據 ICC 之保全性及用 SET 及其他通訊協定所具體實施證書原理(certificate principle)可提供非常高保全性。使用裝置，則在網際網路上沒有銀行秘密及個人秘密之流通，而僅有加密之資料。

裝置之載入能力使得其在本文之諸如 SET保全通訊協定中特別具有多樣性，因爲，如果如 EMV 之新規格或"藍牙(blue tooth)"標準開始使用，裝置可一直相對特定通訊協定來升級，且可以簡單軟體載入來升級。

本發明裝置優點在配合可插入裝置之 ICC 來使用在通訊網路中執行保全交易，但是裝置沒有插入 ICC 也可在通訊網路中執行保全交易。沒有使用 ICC 之交易的實例，如電子郵寄加密、及使用者鍵入信用卡資料之諸如信用卡號碼及到期資料的作業，如有需求可連帶提供其他識

五、發明說明（9）

別裝置。甚至當裝置提供有讀卡機時，其可不插入卡而使用裝置用於保全交易。

通常，裝置可使用以通訊網路來用於所有保全交易，包括信用卡及簽帳卡應用、虛擬卡交易如電子錢包(e-purse)(尤其用於在家重新載入電子錢包)、健康卡、電子貿易(e-trade)、電子銀行包括家庭銀行、電子郵寄保全、保全存取個人資料、和公務機關之保全往來(secure dealins)包括電子稅務(e-tax)、電子投票(e-voting)包括公司股東投票、系統中具有固定電話裝置及行動電話之電傳通訊、及用於包括有關防衛及私人存取系統等之限制性存取系統的選擇性存取等。

本發明也揭示一種電腦程式，儲存在電腦可讀取介質之諸如CD-ROM上、或在伺服器上，用於在通訊網路中執行保全交易，根據本發明之裝置經局部電腦應用來連接到網路。本程式包括上述系統殼層軟體及可載入到裝置之非揮發性記憶體內的應用殼層軟體、及可載入局部電腦應用內用於管理局部電腦及裝置間之全部交易的軟體，包括動態鏈接資料庫(DLL)、用於USB管理性及用I/O管理之系統驅動器、用於管理載入作業之可執行檔案及視需要之測試程式。

附圖之簡單說明

在實例所附之概略附圖，其中：

第1圖表示根據本發明之裝置具有ICC讀卡機形式圖式；

五、發明說明（10）

第2圖表示一種經網際網路之用於保全交易的系統概示圖；

第3圖表示軟體架構；

第4圖表示在保全交易中所包含一序列作業之圖示；及

第5圖表示在載入作業中所包含一序列作業之相同圖示。

詳細說明

第1圖概示之裝置是一種讀卡機30，其設計用於執行所有卡作業及應用過程，其必需防止讀卡機之外界。

讀卡機30包含卡介面32、按鍵34、用於顯示在進行中相關保全交易之訊息的顯示器36、DSP微處理器38及包含E^2PROM及RAM之記憶體40。按鍵34及顯示器36構成使用者介面。裝置進一步包括USB介面42，用於經USB連接器46來連接讀卡機到個人電腦，見第2圖。讀卡機硬體連接到PC44做爲USB匯流排(bus)上之高速匯流排驅動裝置。

按鍵34包括一組功能按鍵35及用於鍵入數字0到9之10個數字鍵。讀卡機之功能鍵35例如可包括：語言鍵，用於交換所顯示訊息之語言；轉換鍵，用於顯示貨幣轉換(即法國法朗及歐元)；取消鍵，用於中斷現有交易；修正鍵，用於刪除最後所按鍵(修正所輸入PAN及／或PIN編碼)；及有效鍵，用於接受所輸入PAN及／或PIN編碼及繼續付款過程。進一步功能如有要求可再包

五、發明說明（ 11 ）

括。

系統概述

如第2圖所示，具有所插入ICC31之讀卡機30連接到使用網際網路瀏覽應用(Internet browser application)之電腦44。電腦44之使用者可開啓提供服務或商品之商家50的對話窗口(session)，其購買利用商家銀行52及發卡銀行54之間電子證書交換來控制，例如使用在下文更詳細說明之SET通訊協定。

啓動在商家位址50處之服務，使用者開始參考號碼也指名50之商家位址應用(merchant site application)(MSA)。本作業可連接其他網際網路位址，而開始在許多位址上之對應應用。應用之一送回使用者電腦44稱為"喚醒(Wake-up)"請求，其將啓動在局部電腦44之特定應用(specific application)。應用啓動讀卡機30且管理在讀卡機30及遠端網際網路位址間之交易。當作業完成時，局部應用取消讀卡機30之鏈接(link)且停止。遠端位址在作業之後接收正或負承認(acknowledgement)。

讀卡機30及局部電腦44代表持卡人系統，如SET標準所定義。ICC311及發卡銀行54是發卡系統。商家位址50、其銀行52及連帶付款管道代表取得系統(acquirer system)。

讀卡機30設計以任何電腦應用來使用，通常個人電腦44。讀卡機30使用電腦44之硬碟中所儲存動態鏈接資料庫(DLL)來啓動及呼叫特定介面功能。一旦作業以

五、發明說明（12）

正確方式實施，讀卡機30即執行所請求應用。各應用是獨立性而其軟體可分別地載入記憶體40之E^2PROM內。本模組實施允許讀卡機軟體更新或甚至於升級。

讀卡機30經USB電纜46來連接到電腦44。讀卡機30以局部電腦44來識別。否則，電腦之作業系統在讀卡機30以主電腦(host)來識別後自動地開啓安裝程序。

如上述，使用者啓動商家位址50來載入"喚醒"請求。本輸入檔案致動局部應用，稱爲局部電腦應用(LCA)其管理在局部電腦44上之讀卡機30(參考電腦44在下文中也使用於LCA)。LCA44以動態鏈接資料庫(DLL)來鏈接到讀卡機30，其傳送LCA請求到讀卡機。LCA44也使得讀卡機響應正式化，而經MSA50來將其傳送到付款管道。

當交易終止時，付款管道(商家銀行52)傳送正或負承認訊息到MSA50及LCA44。當其接收到訊息時，LCA44使得讀卡機30停止而且切離(exit)。如果本訊息沒有來到，在LCA44啓動暫停，其在顯示錯誤訊息之後停止讀卡機30及局部應用。

商家位址50對應通常以URL位址來說明之網路位址(Web address)，在其中可購買一組商品。所購買商品可添加到藍子(basket)來做選擇。在選擇結束時，購買者可準備購買指令(command)及選擇付款支援(payment support))(SSL信用卡作業、具有虛擬錢包之卡作業等)。

讀卡機防止受到外部實體(external entity)所攻擊，具

五、發明說明（13）

有下列特徵。

特定應用可根據PC／SC規範來提供自局部電腦44到ICC31之透明指令（transparent command）。然而，一旦電腦44及讀卡機30間已啓動保全交易，則不允許用於ICC31之透明指令。例如，不可能在電腦鍵盤上輸入PAN或PIN編碼，及傳送本資料到讀卡機30來核對。秘密資訊例如PAN及／或PIN編碼總是在傳送到電腦44之前先行加密，反之亦然。靈敏編碼線在寫入讀卡機30之E^2 PROM之前先搜求（scramble）。

保全是根據加密算法（crgptogram algorithms）：計算性能愈高，保全性位準愈高。然而，加密算法之實際限制在於實際時間作業。使用者不接受超過12秒之計算期間。以所述讀卡機，加密算法可在少於5秒內來實施。

SET通訊協定具有優點地選擇用於資料管理以便匹配保全要求。SET通訊協定之管理需要硬體及軟體具有下述能力用於I／O緩衝器之大記憶體空間，大於標準使用之4（Kbytes）仟位元，而且用於特別情形可擴充到64Kbytes。I／O緩衝器必需具有彈性管理，因為所有資料可具有不同長度。資料之I／O結構必需以讀卡機之RAM堆陣來管理，其必需大於4Kbytes。其必需有用於大量計算之能力，其需求DSP398具有充分高處理速度。如此需要RAM具有至少16Kwords（仟字）。例如，德州儀器之市售TMS320UVC5402型的DSP可以使用。

訊息真實性編碼（Message Anthentication Code）可使

五、發明說明（14）

用到具有產生私用鍵之RSA編碼(Rivest-Shamir-Adleman算法)的2048位元(Bits)。可提供簽名之散列編碼過程。

讀卡機30使用低成本DSP及E^2PROM是非常低成本，而且堅固及易於安裝。使用者不可以執行錯誤操作來刪除基本資料。

考慮本發明尤其針對具有多重功能而經常修改之銀行市場區隔(banking market segment)，軟體可能變得很快地作廢。因而，讀卡機30設計成爲具有載入功能。僅有基礎軟體保留在讀卡機30內。驅動軟體(Drivers)(用於卡31、按鍵34等)、資料庫(ASN.1訊息等)、系統殼層及全部應用是可載入。如此需要下述能力。提供大的E^2PROM記憶體預留允許所載入軟體之舊版本緩衝。在載入作業中斷之情形中，重新啓動來重新安裝舊版本。載入功能必需由LCA44或使用者請求之外部應用來觸發。而且，軟體在寫入記憶體內之前必需控制。

爲資料之保護，一些基本資訊必需防止被外人所讀取。爲此目的，一部份RAM在不可讀取區內。

讀卡機30連同DLL來提供API給使用者應用，而USB驅動軟體用於DLL和系統之驅動堆疊(systems driver stack)來通訊。其也具有可執行軟體，其管理韌體(firmware)載入到讀卡機，及測試程式其實施工廠測試。本PC軟體配備讀卡機例如用於視窗之9872000平台(platform)。在測試結束時，讀卡機接收不能去除之簽

五、發明說明（15）

名。

當系統認知新USB裝置時，DLL在讀卡機安裝期間自安裝CD來拷貝到PC硬碟，而且如使用者應用所要求地載入。API對使用者應用包含三種功能來開啓、讀取／寫入及關閉讀卡機30。在DLL中有執行多加功能(非API)而在其作業中來輔助讀卡機。方塊導向非同步(block oriented asynchronous)半雙通傳輸通訊協定已定義來傳送在DLL及讀卡機30間之資料。

當系統認知新USB裝置時，USB驅動軟體(隨讀卡機30來供應)在讀卡機安裝期間自安裝CD來拷貝到電腦硬碟，而且當讀卡機連接到USB匯流排時，如系統所要求地載入。DLL經USB驅動軟體和讀卡機30來通訊。

E^2PROM連同USB連接之使用具有優點在讀卡機30可以主電源供給器來作業，而不需要電池。

當系統認知新USB裝置時，載入可執行軟體(隨讀卡機30來供應)在讀卡機安裝期間自安裝DC來拷貝到PC硬碟。當使用者或遠端地址應用傳送載入請求時，由LCA(經DLL)來執行。本載入有關更新韌體必需自網際網路地址來傳送到讀卡機內。在本作業期間，PC屏幕上所出現視窗顯示傳送進度及狀態。

工廠測試程式提供用於在讀卡機30組裝後之測試。本程式實施讀卡機(USB、顯示器、按鍵、卡插入)基本功能核對，而且寫入其快閃記憶體(flash memory)(E^2PROM)來自讀卡機30上之條碼標籤的編碼序號。

五、發明說明（16）

軟體

讀卡機30內所安裝軟體基本上以目標導向程式語(objeet ariented programming language)之諸如C及C++來寫入。但是讀卡機處理器38是DSP，僅解讀彙編指令(assembler command)。因此理由，源檔案(source file)首先利用C／C++編譯器在彙編器(assembler)解讀。一些減緩性能之重要功能在彙編器中來最佳化，例如在PSA計算期間所需要之功能。

第3圖表示軟體架構。讀卡機軟體60內建在三個主殼層內，啓動殼層62、系統殼層64及應用殼層66。啓動殼層62對應基礎軟體(ground software)其管理軟體載入；本殼層決不能載入。系統殼層64，其可載入，對應管理應用殼層之其他作業系統。應用殼層66，也可載入，包含管理諸如付款申請之應用。

如圖示說明，啓動殼層62包含USB管理軟體，及用於管理載入之全部軟體，包括使用於載入之RSA／DES管理軟體。可載入之系統殼層64包含使用爲I／O解讀器、RSA及DES加密／解密工具及如卡、鍵盤及顯示管理之驅動軟體的ANS.1資料庫。可載入之應用殼層62包含例如終端機識別應用及載入應用之行政應用。其也包含ICC應用，即用於各晶片卡之一組應用，例如控制不同付款型式，例如使用EMV參數之付款、或預付卡付款或所謂Mondeo付款。

當USB電纜46連接到電腦44時，DSP38接上電源。

五、發明說明（17）

其開始運轉及輸入啓動殼層62，其中執行所有基本啓動程序。本程序基本上核對系統之有效性及致動USB匯流排連接。然後，讀卡機30等待來自LCA44之開啓請求。

一旦LCA44已攻動讀卡機30，DLL即傳送訊息到讀卡機30。視請求之型式而定，訊息在啓動殼層62中管理或傳送到系統殼層64，而且由系統殼層來管理，或傳送到應用殼層66。

啓動殼層軟體62從不能升級。在一實施例中，僅系統及應用能一起升級。在另一實施例中，系統及應用可分開升級。

啓動殼層62、系統殼層64及應用殼層66各具有其版號(version number)。硬體版號寫在讀卡機30之電子平板上。因爲本版號在製造期間已知，所以在啓動軟體中報告其在製造過程結束時安裝。因此，新硬體版號令(nH+1)對應新啓動版號(nB+1)。如果啓動殼層62之修正很微小而新啓動版號可共容前系統版號，則新啓動版號將保持同一型式號碼。因而新啓動版號不會總是造成新型式版號。硬體、啓動及系統版號在升級之後號碼分別是(nH+1)、(nB+1)及(ns)。

如第二實例，實際硬體保留，但所安裝啓動殼層修改。本修改改變系統，即能以實施視啓動版號來執行特定功能之交換而考慮兩種不同啓動版號。本情形中，在升級結束時，硬體、啓動及系統版號分別爲數(nH)、(nB+1)及(ns+1)。因爲新系統版號仍可共容舊啓動殼層，新系

五、發明說明（18）

統將以載入伺服器來整合成新軟體版本，所以前型式號碼保持。

如果啓動殼層修改很重要使得不再可共容現有系統殼層64版號，新系統版號將對應新型式號碼。新系統版號將不會載入前系統殼層做爲新版號。本情形中，新型式號碼分別保持。系統及應用殼層64、66不再共容，而必需以載入伺服器來選擇。當然產生新型式具有缺點在用於各型式需要分離及獨立釋出支援。如此對使用者完全透明，但對製造者有缺點。

當硬體修改需要修改啓動殼層62，其不改變現有或前系統及應用殼層64、66之相容性(例如讀卡機之盒子顏色修改)時，不需考慮爲新型式，但是爲不需要由載入伺服器所特定維護之新子型式。

啓動62或應用64殼層之升級通常導致系統殼層66之升級。但是一些升級不需要系統升級。因此系統殼層仍然和其他殼層無關。如果對其他殼層之修改改變系統殼層66，將產生新系統版號來對應控制組織所發行之新應用識別子版號。

如同系統殼層66，應用殼層之升級仍無關於其他殼層及其他應用。應用總是各自獨立無關。應用升級總是產生新應用版號。如果應用修改對應規範升級，則產生新應用識別主版號。如果其對應內部(製造商)升級，則僅發行組織之識別子版增號。

啓動殼層62所包含編碼基本上啓動DSP38而且核對

五、發明說明（19）

有效系統是否出現。如果是，其開始顯示器按鍵及卡處理過程。如果不是，讀卡機30等待約5秒鐘，然後，以重新安裝其備份拷貝來恢復前系統。然後，本程序啓動USB連接46，且當USB核對完成時顯示"讀卡機準備好了"。同時，讀卡機程式進入所對應狀態機器之無限迴路(infinite loop)，其中下述事件可產生狀態改變：來自DLL之輸入訊息（經USB42）；使用者按鍵（按鍵34）；卡31之插入（卡I／032）。該全部事件以中斷向量(interruption vector)來管理。

在啓動殼層62中，卡I／O僅使用來檢測卡之插或移除。編碼在啓動殼層62呼叫下述功能時進入系統殼層64：

啓動主系統	開始及啓動系統殼層64
顯示系統管理	管理在殼層62內之訊息的顯示
主系統	傳送輸入訊息到系統殼層64
停止主系統	停止系統

第一及最後功能控制系統殼層64之執行。第二功能提供可升級之訊息資料到啓動殼層62。主系統功能控制全部到系統之存取，其根據輸入訊息型式來作業。可輸入系統殼層之訊息分為4個分類，ASN(Abstract Syntax Notation)(抽象語法符號)框訊(frame)；測試請求；

載入應用請求；及互補請求。

輸入訊息根據ASN規範來編碼而解碼，且視其指令頭標題(command header)而由應用殼層66來處理。可用之

五、發明說明（20）

應用殼層在下文中說明。

用於各應用殼層有三個輸入點功能，其允許來啓動、實施及關閉應用。在I／O訊息之ASN結構內所傳送之全部資料是由系統殼層64來管理。該資料在系統殼層64中分配（ allocation ）及集中(deallocation)，但是在應用殼層66內來管理。特定於應用殼層之資料在應用殼層66之內側分配及集中。

測試請求有關製造商來確定讀卡機執行適當。載入應用請求以啓動殼層62來管理，但是用於觸發載入應用及其錯誤管理之請求必需可載入。因此，應用之部份在系統及在應用殼層64、66內實施。一些特定應用請求是由系統殼層64來管理，顯著地來管理連帶大量I／O框訊之管理問題。應用由系統殼層64來呼叫。定義上，應用必需相互獨立無關，其可自啓動及系統殼層來獨立；而且以三種衍生功能來呼叫，其係用於：

啓動：　在處理過程中所需要資料結構之分配，資料之起始及控制應用過程之變數設定

處理過程：　應用步驟之非方塊或方塊處理

終止：　應用資料結構及最後處理過程之集中，如顯示清除或卡移除之請求

例如，擬想兩個應用之實施；行政應用，其管理讀卡機識別及軟體載入請求；及付款應用，其實施用於特定型式智慧卡之付款作業。

一旦載入作業開始，即在E^2PROM之備份或緩衝區內

五、發明說明（21）

拷貝前系統或／及應用區，而且刪除。在本作業期間，按鍵34及卡I／032去致動，而讀卡機30在36處顯示訊息"下載中，請等待"。在載入之前，讀卡機30製備其ASN.1答覆。其以系統殼層64內所呼叫兩個功能來實施。第一功能製備LCA44所期望之正確答覆，其包含在讀卡機載入過程結束時資料庫必需以LCA44來載入時之DLL檔案的路徑（path）。第二功能包含在錯誤情形中必需回送之錯誤訊息。

保全交易處理過程

第4圖說明一種保全交易，諸如以介面裝置內之ICC來執行付款，即讀卡機30使用局部電腦44做為LCA錢包，經網際網路和在商家地址MCA50處之商家來通訊，而付款管道55例如使用SET通訊協定。在第4圖中，號碼1至21使用來指名交易之連續步驟，包含下步步驟：

步驟1-3：讀卡機識別

使用以啓動商家位址50來載入喚醒請求為步驟1，而在步驟2中提供輸入檔案使得LCA44傳送用於讀卡機識別RIDReq之請求到讀卡機30。各讀卡機30以其啓動殼層62內所包含之編碼序號來識別。在步驟3中如果所識別讀卡機30連接，則承認／響應RIDRsp回送到LCA44。

步驟4-7：ICC識別

在步驟4中，LCA44傳送卡識別請求CIDReq到讀卡機30，其在步驟5中傳送本請求到ICC31。讀卡機30內所插入ICC31之識別使用ICC之內部處理器來產生，即

五、發明說明（22）

不使用在讀卡機30內所載入之加密／解密工具盒。一旦ICC31識別，即在步驟6及7中回送接受訊息CIDReq到LCA44。在本ICC識別過程中，讀卡機30作用為一"視窗"；全部必需加密／解密作業在ICC31及在LCA44內發生。

CIDReq要求ICC識別，而且也恢復初始付款參數。本指令以LCA44來使用獲得用於建立付款請求初始訊息所需要之付款參數。

步驟8-17：付款交易

然後，在步驟8中，自LCA44來傳送付款初始請求PinitReq到商家地址50，而且在步驟9中伴隨必需之證書(certificates)回送到LCA44。通常在本付款初始請求PinitReq之後跟著付款請求PagReq，因此當其完成時沒有顯示請求卡移除之訊息。在本請求處理期間之錯誤將中斷付款程序，而且在36處顯示邀請卡移除之訊息。

在步驟10中，LCA44傳送付款請求PayReq到讀卡機30。PayReq要求讀卡機30實施付款處理過程。當讀卡機30接收此一請求時，其不能執行另一作業，直到付款申請案完成為止。PayReq要求讀卡機30實施以卡簽名來保全之交易。經由本指令，電腦44接收資料及資訊，其可顯示及回送加密敏感資料到管道55。

在步驟11及12中付款作業在讀卡機30及卡31間執行。在本步驟，讀卡機30核對卡31是否已插入。如果沒有，則要求卡插入。然後其核對所插入卡是否對應

五、發明說明（23）

前在CIDReq作業已識別之一。如果不是，錯誤訊息顯示說明卡無效，而付款程序中斷。

在本初始步驟之後，讀卡機30顯示所要扣除（debit）之金額，而且要求使用者輸入他的／她的PIN編碼。以輸入及確認有效PIN編碼，使用者接受付款交易條件。讀卡機30確認正確PIN編碼輸入及實施保護計算。然後，在步驟13中讀卡機30傳送付款請求PRsp到LCA44。在本指令結合時，在步驟14中LCA44接收以保護框訊所加密之全部敏感資料，其包括在傳送到MCA50之付款請求訊息PReq。如此，沒有敏感資料在局部電腦44上可讀取或傳送到網際網路內。

在步驟15中，MCA50提供必要之證明且將其包括在傳送到付款管道55之授權請求AuthReq。在步驟6中，付款管理55具有必要之鍵使得所提供加密卡識別資料解密，而且在步驟17中，MCA50傳送付款請求PRes到LCA44，如此付款請求可在LCA上實施。

在付款處理過程結束時，卡31可移除。如果在PRS之後傳送互補請求ComplReq(見下文)，則讀卡機30不要求卡移除。在進一步付款處理期間，甚至當錯誤發生時，在顯示器36上顯示不同訊息。錯誤中斷付款交易而且讀卡機30要求卡移除。

步驟18-21進一步處理過程

在付款交易之後，讀卡機30可經由ComplReq之指令來要求實施進一步處理過程。付款管道55例如以啓動載入

五、發明說明（24）

請求及／或顯示在局部電腦屏幕上已知訊息，可請求讀卡機30之軟體升級。

軟體載入

第5圖表示軟體載入順序。在圖示中，號碼1至8使用來指名載入順序之連續步驟。第5圖之步驟2在ComplReq用於軟體載入之情形中可視為等於第4圖之步驟22。本情形中，喚醒對應在PRes17響應中所包含之完整訊息。

在步驟1'中響應喚醒，LCA44在步驟2'及3'中和MCA50交換載入請求DownloadReq，而使得軟體載入到LCA544。在步驟5'至8'中，DWNReq在LCA44及讀卡機30之間交換，致使軟體載入到讀卡機30。

軟體載入應用是利用控制組織所產生私鍵而計算之PSA簽名來保護，其以本鍵來證明在讀卡機30內側之軟體合格於實施根據所選擇保全通訊協定之付款交易。

記憶體可允許用於所要一起或分離地載入之應用及系統，所要入之檔案集合在單一檔案內，其檔案名稱對應讀卡機30之指名。

如上述，讀卡機30之E^2 PROM緩衝區做為緩衝記憶體，用於在載入作業期來暫時儲存主動E^2 RPROM所傳送系統及／或應用軟體。如果載入作業中斷或失敗，則啓動信號來重新載入軟體。

安裝

因為讀卡機30以特定驅動軟體及局部電腦應用軟體

25

五、發明說明（　）

(LCA)來控制在局部電腦44，所以安裝程序以兩個步驟，驅動軟體安裝及LCA安裝，例如使用容納所要載入電腦內之軟體的CD-ROM。

軟體升級

通常，在標準交易結束時軟體自動地升級，例如付款。系統使用讀卡機30連接到管理伺服器(management server)之事實，用於核對在讀卡機30內所安裝之實際軟體版號。如果版號低於在伺服器上之現有者，則其傳送輸入請求到讀卡機30，如上述。使用者也可獨立地請軟體載入。

讀卡機30設計經USB連接42／46來附接在PC。然而，其不僅提供智慧卡作業，也是用於加密算法之強大工具。因為卡31及讀卡機30和PC44分離，讀卡機30提供有用的工具用於保全在PC上所承攬之交易。讀卡機30之系統及應用軟體是可載入，任何應用軟體也可開發且載入讀卡機30內。本應用可使用在讀卡機之載入系統軟體內可用之工具資料庫。

讀卡機30之進化是鏈接到其軟體架構，其如上述是根據三個殼層模式來建立。第一殼層之啓動殼層62是固定在所設定讀卡機30內側。在製造過程後，啓動殼層62在讀卡機30內不再修改。在啓動殼層62上是系統殼層，其包含包括加密／解密功能之工具盒。系統資料庫之功能共容於全部的啓動功能，而不限在同一型式號碼內之啓動版號。大部時間，本殼層64之升級提高全

五、發明說明（26）

用之升級。換言之，讀卡機30將完全地升級(系統及應用殼層64、66)。

應用開發使得其等各自獨立，但僅由系統殼層64及／或可能由啓動殼層62而來。本最後相關性(dependence)在可能範圍必需避免。新應用總是需要系統升級。但是其從未要求大幅之啓動升級，因爲其意指將需要產生新讀卡機型式，共容於本新應用軟體。系統殼層升級鏈結輸入點導入到新應用軟體。

因此，當新應用軟體第一次載入時，系統也必需同時載入。然後，應用可分開地載入。如此將減少用於單一應用升級之載入期間。如果應用軟體變成過時作廢時，其可能：

- 升級本應用。通常其對應分離載入應用。有時系統必需同時更新。
- 以另一應用來替換應用。如此並不意指系統將載入新軟體，因爲前應用之輸入點可再使用。
- 刪除應用。其意指輸入點將刪除，所以系統必需載入。

當已知組織之付款應用整合在現有軟體內時，組織必需核可讀卡機30。其軟體由組織來簽署；控制載入作業之私用鍵是組織所有。本程序將選擇用於任何應用，其需要讀卡機完整性(integrity)之特定核可。因此，有單一共用鍵(public key)控制軟體載入，所以僅有一個特定外部組織可控制軟體完整性。

在讀卡機製造過程之後，軟體之任何修改必需載入。

五、發明說明（27）

因爲軟體必需正確地簽署而爲讀卡機30所接受，具有載入私用鍵之所有權的外部組織能控制及核可新軟體之完整性及品質。甚至如果軟體修改對應增加之新應用而完全和其本身應用無關，外部組織能控制新添增應用實際上不改變其保全應用。本特徵之優點在外部組織控制私用鍵，其總是保持在讀卡機內所載入軟體之控制。

由上可見本發明已提供多用途裝置來確保對使用者之完全保全，而且其可整合在現有或未來所導入通訊網路中之保全交易的通訊協定內，尤其在擁有讀卡機私用鍵的組織控制下。更進一步，所述讀卡機可使用於許多其他有或沒有插入卡之保全交易，包括電子銀行、電子稅務、保全電子郵寄、電傳通訊及限制存取系統。對上述硬體及軟體之實例可實施許多修改而沒有脫離本申請專利項目之範圍。

符號之說明

30 讀卡機

32 卡介面

34 按鍵

35 功能按鍵

36 顯示器

37 數字鍵

38 DSP微處理機

40 記憶體

42 USB介面

五、發明說明（28）

44 個人電腦

46 USB 連接器

50 商家位址

52 商家銀行

54 發卡銀行

55 付款管道

60 讀卡機軟體

62 啓動殼層

64 系統殼層

66 應用殼層

A5
B5

四、中文發明摘要（發明之名稱：　用於在通訊網路中執行安全交易之裝置　）

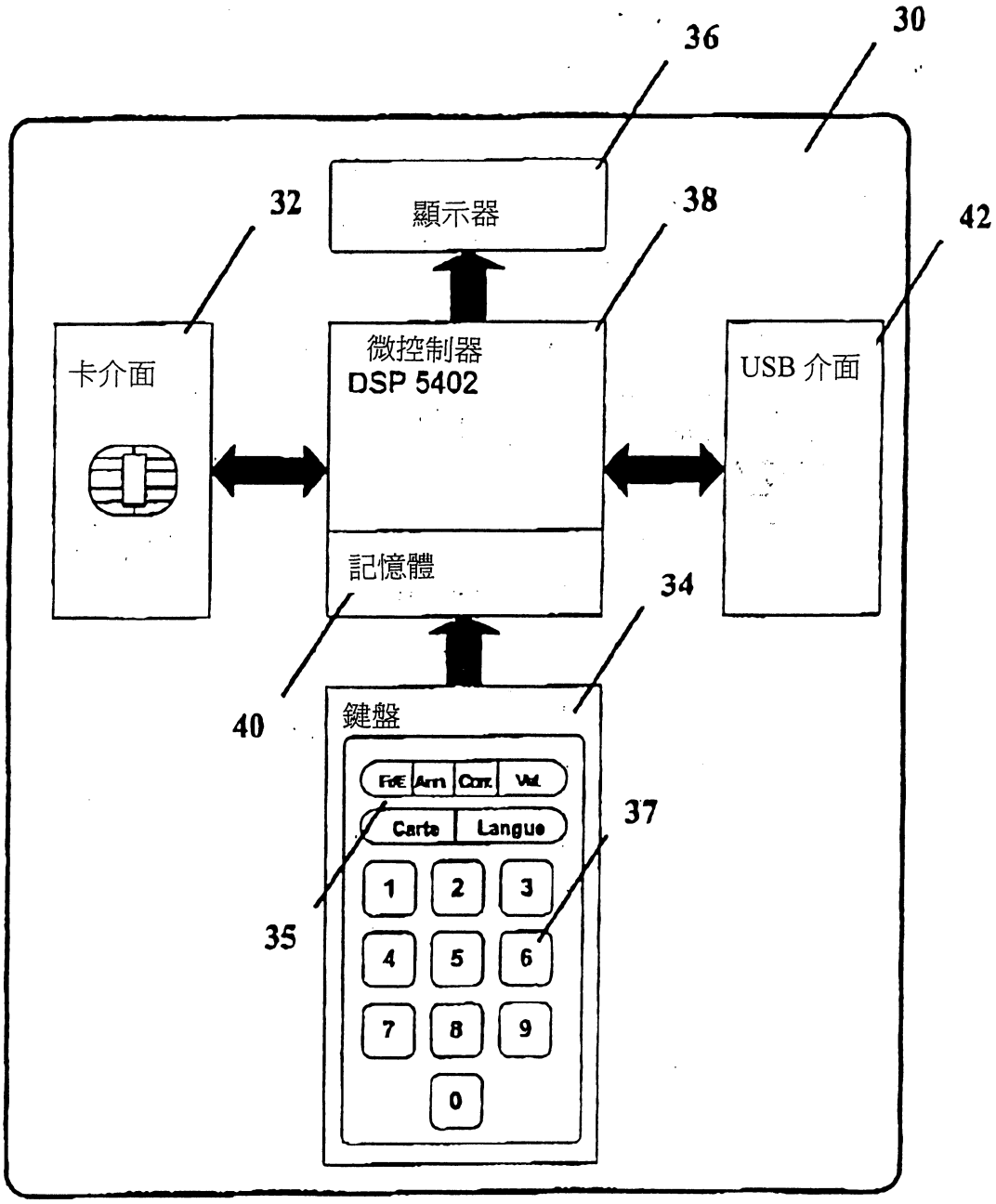
一種裝置，尤其可連接通訊網路之諸如網際網路做為終端機的讀卡機（30），用於使用通訊協定之諸如SET來執行保全交易，包含按鍵（34）、用於顯示關於進行中之保全交易訊息的顯示器；DSP微處理器（38）及包含非揮發性記憶體及RAM之記憶體（40）。非揮發性記憶體配置來儲存軟體在三個殼層內，啓動殼層（62）、系統殼層（64）及應用殼層（66）。啓動殼層包含不可載入基礎軟體，其管理軟體載入到系統殼層及應用殼層內。該裝置連同可載入系統殼層軟體及應用殼層軟體，一個應用配置來瞬時儲存經該按鍵（34）所鍵入PAN或PIN編碼在RAM之網路不可存取部份內；加密該編碼及輸出所加密編碼到通訊網路。該裝置可使用於電子商務、電子銀行、電子稅務、電子郵寄、電傳通訊及限制存取系統等之保全交易。

A5
B5

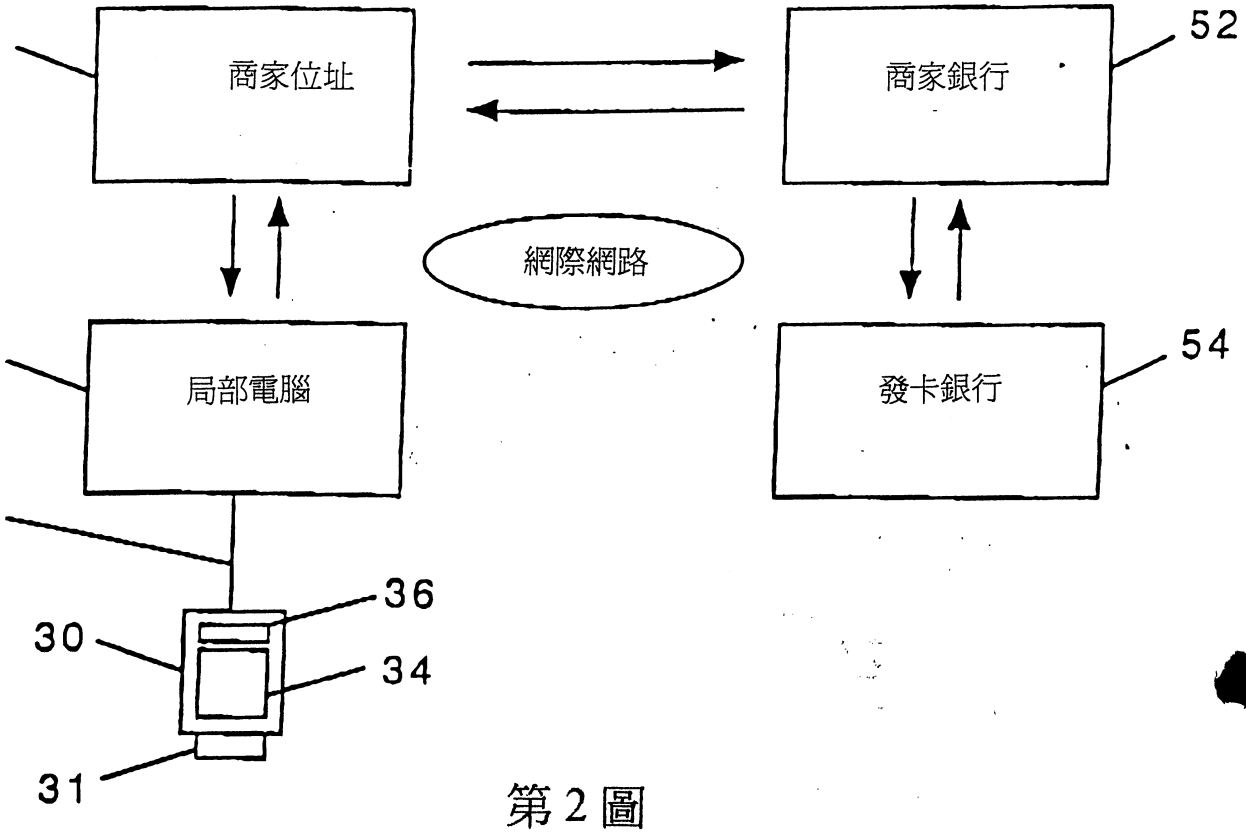
四、英文發明摘要（發明之名稱：　　）

Device for carrying out secure transactions in a communications network

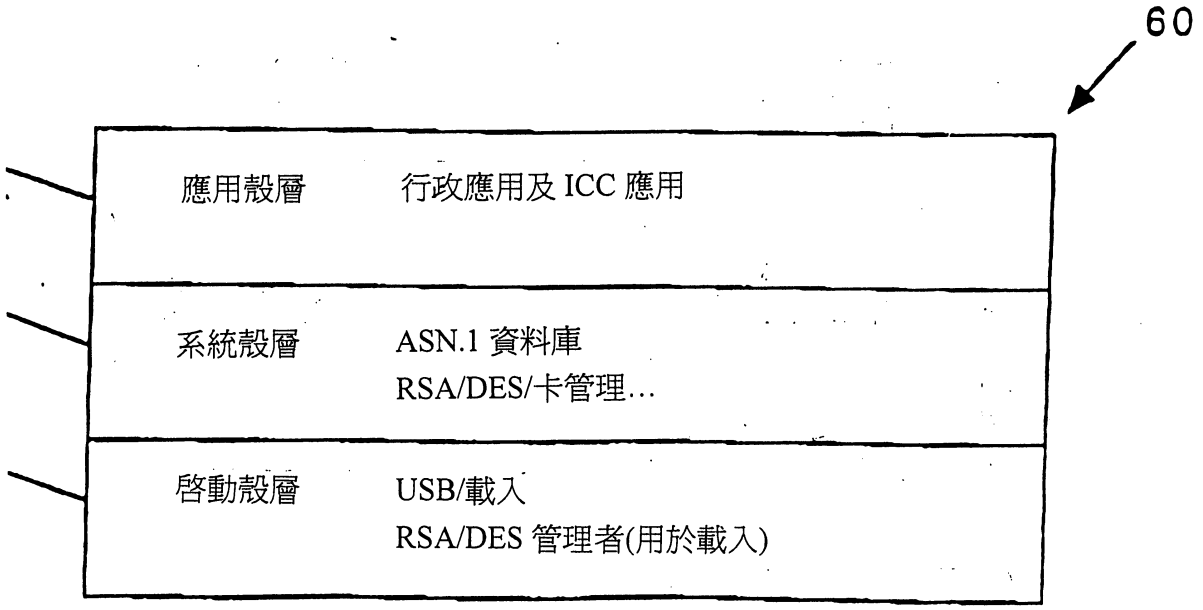
A device, in particular a card reader (30) connectable as a terminal of communications network such as the Internet for carrying out secure transactions, in particular using a protocol such as SET, comprises a keypad (34), a display (36) for displaying messages related to a secure transaction in progress, a DSP microprocessor (38) and a memory (40) comprising a non-volatile memory and a RAM. The non-volatile memory is arranged to store software in three shells, a boot shell (62), a system shell (64) and an application shell (66). The boot shell contains non-downloadable ground software that manages software download into the system shell and the application shell. The device is associated with downloadable system shell software and application shell software, one application being arranged to momentaneously store in a network-inaccessible part of the RAM a PAN or PIN code keyed in via the keypad (34); encrypt the code and output the encrypted code to the communications network. The device is useful for secure transactions in e-commerce, e-banking, e-tax, e-mail, telecommunications and restricted access systems, etc.


36
30
32
顯示器
38
42
卡介面
微控制器
DSP 5402
USB 介面
記憶體
34
40
鍵盤
Carte
Langue
37
35
1
2
3
4
5
6
7
8
9
0

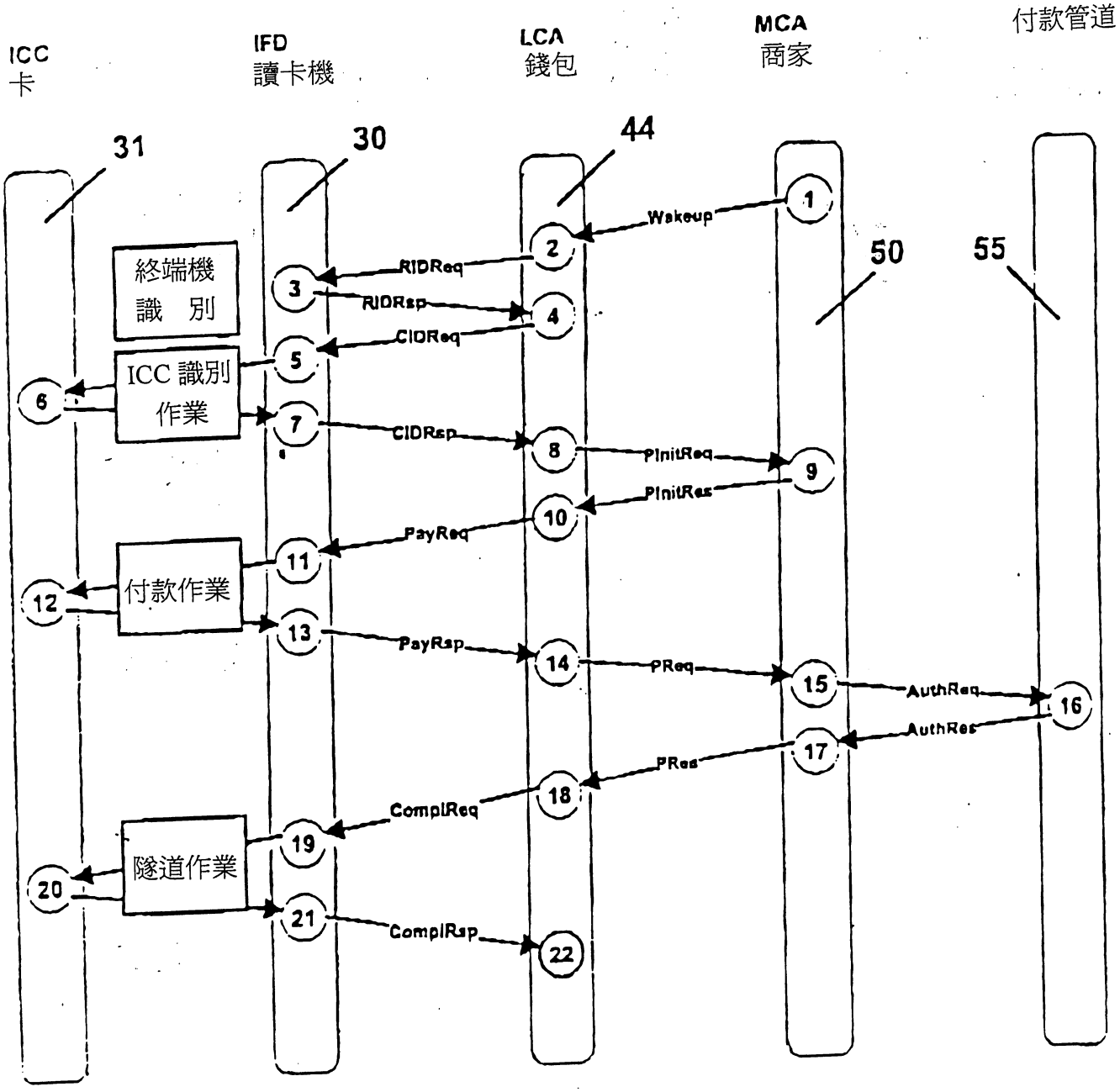
第 1 圖


商家位址
商家銀行
52
網際網路
局部電腦
發卡銀行
54
36
30
34
31

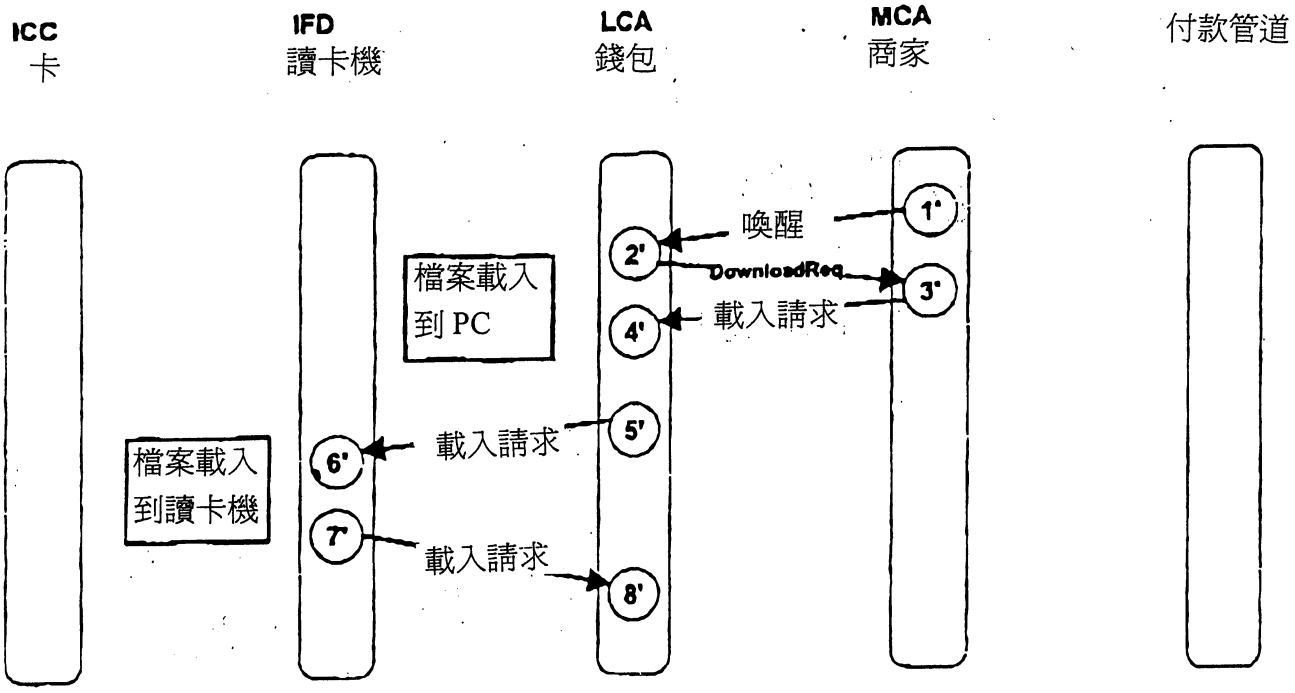
第 2 圖


60
應用殼層
行政應用及 ICC 應用
系統殼層
ASN.1 資料庫
RSA/DES/卡管理…
啓動殼層
USB/載入
RSA/DES 管理者(用於載入)

第 3 圖


ICC
卡
IFD
讀卡機
LCA
錢包
MCA
商家
付款管道
31
30
44
50
55
終端機
識 別
ICC 識別
作業
付款作業
隧道作業
Wakeup
RIDReq
RIDRsp
CIDReq
CIDRsp
PInitReq
PInitRes
PayReq
PayRsp
PReq
PRes
AuthReq
AuthRes
ComplReq
ComplRsp
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22

第 4 圖


ICC
卡
IFD
讀卡機
LCA
錢包
MCA
商家
付款管道
喚醒
DownloadReq
載入請求
檔案載入
到 PC
檔案載入
到讀卡機
載入請求
載入請求
1'
2'
3'
4'
5'
6'
7'
8'

第 5 圖

577000

92年11月7日 收

六、申請專利範圍

第 89117790 號「用於在通訊網路中執行安全交易之裝置」專利案　　（92 年 11 月修正）

六、申請專利範圍：

1. 一種可連接做爲通訊網路終端機來用於在網路中執行保全交易之裝置，尤其連接電子商務、電子銀行、電子郵寄、電傳通訊及限制存取系統，該裝置包括：

按鍵，用於顯示有關在進行中之保全交易訊息的顯示器，微處理器及配置來儲存在三個殼層之啓動殼層，系統殼層及應用殼層內的軟體，其中該啓動殼層包含管理所載入在該系統殼層及該應用殼層內之軟體的非可載入基礎軟體；

該裝置連同可載入或所載入在記憶體內之軟體，即是：

- 系統殼層軟體，包含管理該應用殼層、ASN 資料庫及加密／解密工具盒之軟體；及
- 應用殼層軟體，包含管理用於保全交易應用的軟體，包含所配置之應用，當軟體載入在該記憶體內而該裝置連接到通訊網路時，在該裝置內使得經該按鍵所鍵入編碼加密及輸出所加密編碼，而不用可自該裝置外側來存取之鍵入編碼。

2. 如申請專利範圍第 1 項之裝置，其中該應用配置來內部地執行該裝置之下述作業：

煩請委員明示 92 年 11 月 7 日所提之修正本有無變更實質內容是否准予修正。

六、申請專利範圍

- 瞬時儲存經該按鍵所鍵入編碼在該記憶體之網路不可存取部份內；
- 加密該瞬時所儲之鍵入編碼，而在一加密之後即將其自該記憶體來刪除；及
- 自該裝置內輸出該加密編碼到通訊網路。

3. 如申請專利範圍第 1 項之裝置，包含用於 ICC 卡之讀卡機，該裝置配置使得在隨後所插入該讀卡機之 ICC 上能夠卡識別及接受，如果卡被接受，以該作業來建立交易接受。

4. 如申請專利範圍第 2 項之裝置，包含用於 ICC 卡之讀卡機，該裝置配置使得在隨後所插入該讀卡機之 ICC 上能夠卡識別及接受，如果卡被接受，以該作業來建立交易接受。

5. 如申請專利範圍第 3 項之裝置，其中該卡識別及接受作業及／或該交易接受作業中之至少一部份，是利用併合在該裝置內所插入之 ICC 的處理器來實施。

6. 如申請專利範圍第 4 項之裝置，其中該卡識別及接受作業及／或該交易接受作業中之至少一部份，是利用併合在該裝置內所插入之 ICC 的處理器來實施。

7. 如申請專利範圍第 1 至 6 項中任一項之裝置，其中該記憶體包含緩衝區，其使用做爲在載入作業期間

六、申請專利範圍

來暫時儲存前載入系統及／或應用軟體之緩衝記憶體，該記憶體連同裝置響應顯示載入作業中斷或失敗的信號，用於重新載入系統及／或應用軟體。

8. 如申請專利範圍第 1 至 6 項中任一項之裝置，其中該記憶體包含非揮發記憶體，尤其 E^2PROM，用於儲存可載入之讀卡機；及 RAM，其包括該記憶體之網路不可存取部份。

9. 如申請專利範圍第 1 至 6 項中任一項之裝置，併合在：(a)可連接到個人電腦之手持式外部讀卡機；(b)可連接到個人電腦之個人電腦的分離鍵盤；(c)可攜式個人電腦；(d)數位電視接收機之視訊選擇盒；(e)固定之電話機；(f)行動通訊裝置之諸如行動電話；或(g)銷售點之販賣裝置。

10. 一種用於在通訊網路系統中執行保全交易之持卡系統，包含如申請專利範圍第 1 至 6 項中任一項之裝置，連同局部電腦應用(LCA)之諸如 PC，該裝置較佳地以 USB 連接器來連接到 PC。

11. 如申請專利範圍第 10 項之持卡系統，其中該 LCA 儲存軟體，包括用於管理在該局部電腦及所連接裝置間之全部通訊的動態鏈接資料庫(DLL)。

12. 一種通訊網路，其中加密資料在發卡系統、商家位址應用、付款管道及如申請專利範圍第 1 至 6 項中任一項之裝置、或如申請專利範圍第 10 或 11 項之

六、申請專利範圍

持卡系統間來通訊，其中該裝置連接到該通訊網路來形成用於在該網路中執行保全交易之終端機。

13. 如申請專利範圍第 12 項之通訊網路，其中該發卡系統、商家位址應用、及付款管道根據通訊協定之諸如 SET 來交換電子證書。

14. 一種可電腦讀取媒體，用以在通訊網路中執行保全交易於經局部電腦應用軟體連接到通訊網路之如申請專利範圍第 1 至 6 項中任一項之裝置，包含該系統殼層軟體及可載入該裝置之記憶體內之應用殼層軟體，以及可載入該局部電腦應用殼層內之軟體，用於管理在該局部電腦及所連接裝置間之全部通訊。