

公告本

申請日期	88.10.27
案 號	88122702
類 別	HWL 12/00, HWL 8/82

A4
C4

510098

(以上各欄由本局填註)

發明專利說明書

一、發明 名稱	中 文	經由網際網路式網路而與伺服器通信所用之配備有晶片卡讀卡機之保全終端機
	英 文	Security terminal equipped with a chip card reader used for communication with a server via the Internet type network
二、發明 創作人	姓 名	瑞努馬瑞納 Renaud MARIANA
	國 籍	法國
	住、居所	法國利卻斯內 78150 拉斯凱什斯廣場 5 號
三、申請人	姓 名 (名稱)	布爾第八特許公司 Bull CP8
	國 籍	法國
	住、居所 (事務所)	法國 78430 路文西納斯第 45 號 郵政信箱伯薩里斯路 68 號
	代 表 人 姓 名	米契爾可倫貝 Michel Colombe

(由本局填寫)

承辦人代碼：
大類：
I P C 分類：

A6
B6

本案已向：

國（地區） 申請專利，申請日期： 案號： ☒有 ☐無主張優先權
法
1999 年 10 月 28 日 99 13508 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

經濟部智慧財產局員工消費合作社印製

五、發明說明()

本發明是有關一種終端機結構，更特別是一種形式的終端機，其使用位於保全牆中的鍵盤與晶片卡讀卡機，並且其目的在於經由網際網路式網路而與伺服器通信。

一個此種裝置是例如在商業名稱“安全墊”(“safe pad”)下為所熟知。

在本發明的範圍中，“終端機”這名詞應該在一般的意義中來瞭解。上述的終端機可以尤其是由在各種不同的執行系統，例如是 WINDOWS 或 UNIX（此兩者均設置標記）之下所運作之個人電腦所構成。它還可以由工作站、手提電腦、或稱為專用的卡片終端機所構成。

同樣地，在本發明的範圍中，“網際網路式的網路”這名詞包括，除了正確地稱為網際網路之外，私人企業或類似的網路稱為“Intranet”，並且此向外延伸的網路稱為“extranet”。

此等晶片卡是使用於各種不同的領域中：醫療銀行應用，像是稱為“電子小錢包”等等。在晶片卡上還可以共同存在數個應用系統（多種應用晶片卡）。

為了此等形式的應用系統，此晶片卡可以有各種不同的功能。尤其是，它可以使用於保全的目的。“保全”這名詞應被包括在一般通常的意義中：尤其是網站使用者及／或晶片卡所有人本身之保密及／或確認。

在更特殊應用系統的範圍中，此終端機可以配備了

五、發明說明 (>)

保全牆其包括一晶片卡讀卡機，一鍵盤以及也許一或多個其他資訊資源。

第 1 圖以概要圖式說明根據習知技術之上述形式終端機之結構。

爲了確定其觀念，假設此終端機 1 是根據微電腦而構成，其配備了此種資訊設備所有通常構成的裝置，並且爲其良好的運作所必需：中央處理單元，活性記憶體 (RAM)，大量記憶體 (硬磁碟)，資訊儲存體 (軟磁片，等) 讀取機，等等。在第 1 圖所描述的特殊情況中，終端機 1 是配備了保全牆 (亦稱防火牆) 3 其包括一晶片卡 2 讀卡機 30，以及一鍵盤 31。此鍵盤 31 特別用於晶片卡 2 持有者確認資料之擷取：其例如是與晶片卡 2 之辨識者有關的口令 (pass word)。各種不同之電子電路允許呈現於此牆中保全元件之間的通信，一方面尤其是鍵盤 31 與晶片卡 2 (經由讀卡機 30) 之間，而另一方面是出現在終端機 1 中的此等保全元件與非保全元件之間。

通常，此終端機在其非保全之部份包括一特殊應用系統 10，其以下稱爲 "交易者"，以確保由在討論中終端機 1 所允許之特殊異動 (transaction) 之管理與控制。此介於應用系統 10 與保全牆 3 之內部元件之間的通信，通常是根據 "RS232" 形式的標準而實施。此保全牆 3 內部元件之間的通信，尤其是常駐應用系統 300，經由讀卡機 30，與晶片卡 2 的通信，通常是根據遵守準則 ISO 9816-1 至 9816-4 之協定而執行。

五、發明說明 (3)

- 此種形式的結構因此呈現不便，尤其是以下：
- 植入於此終端機（非保全部份）之“買主”應用系統，以及植入於保全牆內之常駐應用系統對於此終端機為特殊；
 - 此等有關的資訊程式通常是體積龐大，並且
 - 其靈活性與可靠性是有限，因為修改此等程式須要將程式重新載入於終端機（非保全部份）與保全牆中，以及可能良好功能的測試之執行，其須要特殊人員在場。

通常，此後者作業應對大數目的終端機重覆。

它還應該保有關於全部或部份保全應用系統的精神。其因此應該能夠保證在特定的保全位準更新程式，其適合特殊的應用系統。

往往終端機 1 並不孤立，在此方面它經由傳輸網路 RI，而連接至一或數個遙遠系統，其第 1 圖以一個唯一的 4 說明。網路 RI 的性質根據所設想的應用系統（醫療銀行的應用系統）而可以非常的不同。它可以特別是關於網際網路 Internet 或是 (intranet 或 extranet) 形式之網路，而考慮到此後者形式網路之快速發展以及其要求的應用系統。以通常的方式，此形式的整個結構稱為“主—從”此“從”通常是遙遠系統 4 並且“主”是終端機 1。但是在某些情況中。但是在某些情況中，在交易的時間期間，此等角色可以反過來或者輪換。

在此種結構中，與特殊應用系統 10 與應用系統 300

(請先閱讀背面之注意事項再
為本頁)

裝

訂

線

五、發明說明(4)

有關的程式，不論以任何原因修改版本時，可以由遙遠的伺服器例如伺服器 4，以集中的方式更新。結果是此不方便的信號可以衰減，此項更新可以由電信處理而實施。然而此等作業須要使用良好測試之管理程序。而且，此電傳載入可以包括敏感資料，或者至少不應該允許在終端機中植入不被允許的或是對於保全危險的程式及／或程序（“特洛木馬”、“邏輯炸彈”、病毒等）。

而且，以它配備了網際網路(Internet)式的網路的能力與普遍性，而一方面感覺到此須要將上述之特殊應用系統（其區域性地植入於終端機中），朝遠方伺服器（其以下稱為“伺服器買主”）“遷移”，而另外一方面，從此等伺服器買主與晶片卡直接對話。

此第二項需求，由於以下將說明的原因，尤其不能被習知技術的終端機所滿足。

然而首先，其為有益以簡短描述根據習知技術的系統結構，其允許，經由網際網路(Internet)式的網路 RI，在終端機與遠方伺服器之間的通信。一個此種結構是在第 2 圖上以概要圖式的方式顯示。在此圖上更特別顯示參考號碼為 1'之終端機之軟體結構。

此終端機 1'在此是一般形式的終端機，不論是保全或沒有，其設置對於解釋不同形式通信的原因並不重要。

如同先前所顯示，終端機 1'當然包括其良好運作所需之所有之電路與裝置，並且它不是在設計簡化的目

(請先閱讀背面之注意事項再寫本頁)

裝

訂

線

五、發明說明 (5)

的中呈現。通常，此終端機 1'亦被連接至傳統的週邊設備，不論是否與其整合在一起，例如一顯示螢幕（未圖示）與一鍵盤 31，其位於本發明更特殊領域中之保全牆內（第 1 圖：3）。

通常，在網路上的通信是依據協定符合標準而實施，此標準包括數個重疊之軟體層。在此網際網路 (Internet) 式的網路 RI 的情況中，其通信是根據對此種通信形式特殊的協定而實施，但它亦包括數個軟體層。此通信協定是根據應用而選擇更特別針對："WEB" 網頁之詢問、檔案之傳送、電子郵件 (e-mail 或是根據英文術語 "e-mail")、論壇或 "news" 等。

此等通信網路的結構是由不同的層所描述。作為例子，此 "OSI" 標準 ("開放系統連接"、"Open System Interconnection")，是由 "ISO" 界定，其包括 7 個層，它由稱為底層（例如是稱為 "實體" 的層，它是有關於實體傳輸的儲存體），經由尤其是稱為 "傳輸" ("transport") 層的中間層，而至稱為高層（例如是稱為 "應用" 層）。一個資料層提供服務給直接在其上的層，並且向直接在其下的層，經由適當的界面要求其他的服務。此等層借助於原始軟體件而通信。它們同樣地可與相同位準的層通信。在某些結構中，此等層之一個或另一個可以不存在。

在網際網路的環境中，此等層的數目是 5，並且以更精確的方式而言，從高層至低層是：應用層 ("http"、"ftp"、"e-mail" 等)、傳輸層 ("TCP")、網址層 ("IP")、

(請先閱讀背面之注意事項再為本頁)

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(6)

資料連接層("PPP"、"Ship"等)，以及實體層。

終端機 1'包括至網際網路(Internet)之接達電路 11。它可以是有關一數據機連接至轉接電話線，或者經由例如網際網路服務提供者(根據英文術語，"Internet Service Provider"或"ISP")，而連接至服務整合數位網路("RNIS")。此等接達至網路 RI 的電路 11 重新組合下部軟體層 C₁ 與 C₂，其相對應於上述之"實體"層與"資料連接"層。

同樣地顯示上部層 C₃ 與 C₄，其相對應於"網址"層("IP")與"傳輸"層("TCP")。此上部應用層("http"、"ftp"、"e-mail"等)是藉由任何形式的領航員"WEB"NW 而概括，其較佳是商用標準形式。

此介於低層 C₁ 與 C₂，以及高層 C₃ 與 C₄ 之間的界面，是由通常稱為"底層驅動器"的軟體層 15 所構成。此等支撐於此界面上的高層 C₃ 與 C₄ 是藉由與其相對應之特殊功能程序集或網路程序集 14 而使用，在網際網路的情況中，"TCP/IP"是經由稱為"sockets"之程序集而使用。

此種組織結構允許領航員 NW 向遠方伺服器 4 提出請求，以資詢網頁"WEB"(協定"HTTP")，以便傳輸檔案(協定"FTP")或是傳送電子郵件(協定"e-mail")。

終端機 1'同樣包括在本發明更特別領域內，位於保全牆中之讀卡機 30(第 1 圖:3)。為了與晶片卡 2 通信，讀卡機 30 同樣包括兩個底層 CC1(突體層)與 CC2

五、發明說明 (7)

(資料連接層)，其扮演與層 C₁ 與 C₂ 類似的角色。其與層 CC₁ 與 CC₂ 之軟體界面，是例如由規格 "PC/SC" (" 第 6 部份，service provider) 所描述。此等層本身 CC₁ 與 CC₂ 是特別由準則 ISO 7816-1 至 7816-4 所描述。

一輔助軟體層 13 在應用層 (在獨特的參考號碼 Appli₁ 下)，以及下部層 CC₁ 與 CC₂ 之間形成界面，其主要的功能是歸因於層 13，並且是多路轉換 / 解除多路轉換功能。

從晶片卡 2 這邊，可以重新發現類似的組織，即，出現兩個底層，其參考號碼 CC'₁(實體層)與 CC'₂(資料連接層)，以及界面層 23，其完全類似於層 13。此層 23 確保介於前述協定層 CC'₁ 與 CC'₂，以及一或數個應用層之間的界面，其在獨特的參考模組 Appli₂ 的形式下代表。

此等介於晶片卡讀卡機 30 與晶片卡 2 之間的通信是借助於標準命令而實施，而在英文縮寫 "APDU"(代表 "應用協定資料單元"，Application Protocol Data Unit) 之下而為已知。

可以使用不同的協定，並且作為非窮盡的例子是以下：

- ETS/GSM 11.11 的建議
- 由準則 ISO 7816-3 所界定之協定，在 T=0 的區塊模式中；
- 由準則 ISO 7816-3 所界定之協定，在 T=1 的文字模

五、發明說明 (8)

式中；或

一由準則 ISO 3309 所界定之協定，在 "HDLC" 之框模式中

(其代表 " 高位準資料連接控制程序 " " High-level Data Link Control procedure " 或是高位準連接命令程式) 。

在本發明的範圍中，是較佳使用在區塊模式中之 ISO 7816-3 協定。

以本身所熟知的方式，在每一個協定層，它連接某個數目之原始軟體件，其允許在相同位準的層之間，以及在一層至另一層之間作資料交換。

在此技術之目前狀態中它不能使晶片卡 2 與遠方伺服器 4 經由網際網路 RI 直接通信，因為此剛才所提到之在標準形式之晶片卡 2 之間的通信協定，是與在網際網路上或此種形式所有的網路上所使用的通信協定並不相容。除非在領航員 NW 中植入一特殊形式之稱為 " 插入 " ("plug-in") 之軟體件，它不是不再可能在領航員 NW 與晶片卡 2 之間建立直接的通信。

若重新參考第 1 圖，並假設終端機 1 是連接於網際網路，以及概括剛才所提到的，可以察覺根據習知技術，此終端機 1，其包括一保全牆 3，它配備了鍵盤 31 與晶片卡 2 之讀卡機 30，其包括兩個主要的通信界面 S1 與 S2，其由虛線表示。第一界面 S1，其連接保全牆 3 至正確稱為終端機 1，在那裡執行交易者應用系統 10，以及一第二介面 S2，其用於與晶片卡 2 通

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明(9)

信。事實上，界面 S2 是分佈介於應用系統 300 與晶片卡 2 之間。對此兩個界面還增補了向外的界面（第 2 圖：特別是電路 11），其使得終端機 1 可以與網際網路 IR 通信。界面 S1 接受兩個位準的對話：第一個對話是對於由終端機 1 所發出的指令透明，而由界面 S2 沒有作語義上的修正而執行，以及第二位準的對話其介入應用系統 300。

如此經由在鍵盤 31 上獲得口令 (pass word) 而確認，是一個指令提交給界面 S1，其由應用系統 300 翻譯，並且轉換成一系列之介於應用系統 300 與晶片卡 2 之間的界面 S2 上之交換。此等交換的結果傳送給界面 S1。

不僅此事實，在目前的技術狀態中，它被排除此標準的晶片卡 2 接受直接與網際網路 RI 交換，如同剛才從提到者。根據習知技術此終端機主要的不便是由常駐 (resident) 應用系統的存在所構成。它是更經常關於稱為“所有者”的應用系統，其意味著客戶應用系統 10 應該根據所使用終端機的形式與性質而撰寫。它因此一開始就區別此種終端機的形式與其他終端機的形式，其不方便維護的作業。而且，它適應於網際網路形式的環境。

它建議用於本發明之形式之應用系統的標準，像是在英文縮寫字“OCF”（代表“開放卡片架構”“Open Card Framework”）下所熟知的標準，其有助於介於客戶終端機 1 與晶片卡 2 讀卡機 30 之間交換之標準化，

五、發明說明(一〇)

並例如遵守終端機 "EMV" 準則。然而此種標準在網際網路的本文中不能直接使用。

若同樣的為熟知，在銀行應用的領域中，此稱為 "C-SET" 的協定，此協定是由 G.I.E. 銀行卡片所界定。根據此協定，一使用者在交易者的地點上連接而在 "WEB" 上可以自由地使用，並且進行一項購買。此後者，當在交易時，請求保全牆的元件用以確認執行以購買之銀行卡片之持有者。此項確認是藉由執行在終端機（未保全部份）與牆中的軟體而實施。

- 此協定免除其不便：
- 它使得在終端機與牆內需要存在一特殊軟體；
 - 它使得需要確認此由 "C-SET" 所規定的軟體；
 - 此 "C-SET" 協定是獨特地付款導向：此在終端機中的軟體，其處理伺服器 "WEB" 以及由銀行卡付款的資訊，是一付款軟體。

藉由此等特性，其與先前所提及之習知技術的解決方式沒有太大不同。根據網際網路式的協定，它不允許全部的通信，尤其是晶片卡之直接定址。從其特徵，它不能提供任何的彈性，並且不能調整以使用於其他的領域中：健康、更新儲存在晶片卡上的資料、貸款點等。

這所有是在減輕習知技術方法與結構之不便，並且其部份剛才提過，本發明是確定其目標以滿足其所感覺的需要。

它支持在網際網路上使用此種終端機，其包括一保

五、發明說明()

全牆，此牆配備了至少一晶片卡讀卡機以及一鍵盤，其一方面允許終端機與晶片卡讀卡器之應用系統朝向"WEB"型式的遠方伺服器遷移，而另一方面允許直接與晶片卡對話。

它允許以最大之安全在保全牆內進行更新或附加軟體。

爲了這麼做，根據本發明之第一觀點，晶片卡不再依據前述之通信協定 ISO 7816，藉由"APDU"以傳統的方式定址，而是藉由使用"URL"位址（代表"普遍資源定位"，"Universal Resource Location"），如同其爲所熟知，"URL"位址是由一適當稱作"IP"的位址與埠口(port)號碼所構成。以相同的方式，保全牆使用稱爲"URL"的位址。

根據本發明的一觀點，此晶片卡因此還表現如同伺服器及／或客戶(client)"WEB"。

根據本發明之保全牆是對於網際網路"透明"，在此意義上此由遠方客戶伺服器所發出之"卡片指令"不可干涉到終端機之定址元件。其結果是與此保全牆有關的資源無法由網際網路接達。相反地，包括在晶片卡中的應用系統是可以定址並且啓動在保全牆中所存在的所有的資訊資源，尤其是鍵盤，其如同以下所說明的藉由"URL"而單純地定址。

爲了如此作，此終端機實體上包括：

——一種修正型式的保全牆，其包括至少一晶片卡讀卡機與一鍵盤（及／或另外一個資訊資源），此兩者連

(請先閱讀背面之注意事項再
爲本頁)

裝

訂

線

五、發明說明 (12)

接至一稱為保全牆的伺服器 "HTTP"，以及一執行單元，其管理在此牆內所出現的所有資源，以及一除了傳統式的元件（記憶體等）與 "WEB" 型式的領航員之外，還包括稱為終端機的第一通信節點 (node)，其確保在網際網路，"WEB" 型式的領航員及／或保全牆之間的通信。

另一方面，前述之保全牆包括一稱為牆的第二通信節點，其確保在適當稱謂的終端機，經由第一通信節點，稱為保全牆的伺服器 "HTTP"，及／或晶片卡讀卡器之間的通信。

此晶片卡本身配備了第三通信節點，其稱為卡片，以及一調整軟體，其作用如同伺服器 "HTTP"，其至少在晶片卡中的常駐 (resident) 應用系統與第二通信節點之間形成界面。

此第一通信節點接收了網際網路的請求，其具有朝向此保全牆與此牆有關的埠口號碼，並執行所須的協定調整，以便使得網際網路與第二通信節點直接通信，並且確保資訊及／或指令向晶片卡傳送。

對於某些應用系統，尤其是對於安全水準高要求的應用系統，此保全牆可以有利地包括一個或數個輔助的資訊資源，其例如是生物統計學的確認裝置（眼睛、聲音及／或簽字的辨識），一個共同處理器或一外部的翻譯器。

在一個根據本發明方法的較佳的變化例中，此保全牆之元件與資源之運作或更新所須的程式，是由與此

(請先閱讀背面之注意事項再填寫本頁)

裝
訂
線

五、發明說明(13)

網路相連接的遠方 "WEB" 伺服器，經由網際網路而以電傳的方式載入。此種更新可以包括刪去此等程式之至少一部份。

在另外的實施變化例中，同樣地配備了經由網際網路與通信節點，以電傳下載，將記載於晶片卡中的應用系統或是部份應用系統（檔案、程式、劇本等）更新及／或刪除。

所有此等作業可以在非常良好的保全情況中實施，此上述保全牆對於網際網路透明的事實。

因此本發明的主要目的是提供一終端機，其配備了保全牆，其目的是根據網際網路式的第一通信協定，經由網際網路式的網路，而與至少一個 "WEB" 型式的伺服器通信。該保全牆包括至少一晶片卡讀卡機，該晶片卡至少儲存至少一個應用軟體，其特徵為該終端機包括一非保全部份，該部份至少包括一稱為第一通信節點的第一模組。該保全牆包括至少一稱為第二通信節點之第二模組，並且該晶片卡包括一稱為第三通信節點之第三模組，其中該等通信節點各包括第一、第二、與第三協定堆疊，其各包括一特定數目稱為標準的通信軟體層，以及第一、第二、與第三特殊軟體件，其各包括至少一第一軟體實體，該第一軟體實體是兩個兩個配成對，其中該第一通信節點至少允許根據該網際網路式之該第一通信協定之介於該終端機與該伺服器 "WEB" 之間的通信，其中該第一與第二特殊軟體件之該第一實體，允許根據特定之第二通信協

(請先閱讀背面之注意事項再
為本頁)

裝
訂
線

五、發明說明 (14)

定，在該終端機與該保全牆之間，建立資料雙向交換會議，其中該第二與第三特殊軟體件之該第一軟體實體，允許根據特定之第三通信協定，經由該晶片卡讀卡機，在該保全牆與晶片卡之間，建立資料雙向交換之會議，以便能夠至少使得該晶片卡的軟體應用系統與該"WEB"式的伺服器建立關係。

本發明現在參考附圖以更詳細的方式描述。

圖式之簡單說明

第 1 圖以概要圖式說明根據習知技術之終端機的例子，其包括了配備了一晶片卡讀卡機與一鍵盤的保全牆。

第 2 圖以一般的方式說明根據習知技術之終端機之邏輯結構，其包括一晶片卡讀卡機，並且經由網際網路與伺服器"WEB"通信。

第 3 圖以概要圖式說明根據本發明之一般性結構之例子，其允許經由網際網路，介於稱為交易者之遠方伺服器與終端機之間的通信，此終端機配備了保全牆，其包括了一晶片卡讀卡機、一鍵盤、與其他的資訊資源。

第 4 圖顯示模組的邏輯結構，其允許介於第 3 圖終端機之保全牆與晶片卡之間的通信；以及

第 5 圖顯示晶片卡之邏輯結構之特殊實施模式。

現在藉由參考第 3 圖描述依照本發明之保全牆終端機之實施例，以及介於終端機與稱為"交易者"之伺服器與終端機之間之系統結構。

五、發明說明 (15)

此終端機其以後的參考號碼是 5，如同其所顯示，可以根據微電腦式類似的裝置而實現。它包括某個數目的傳統式元件；微處理器、活的(RAM)與死的(ROM)記憶體、大量記憶體（硬碟等）等，其並未圖式並且為此行業的人士所熟知。相反的，在屬於本發明的應用系統中，終端機 5 包括一保全牆 6，其由本身所熟知的方式，藉由實體與邏輯的方式保全。此保全牆 6 包括與習知技術相同之元件，但是還有對本發明特殊的元件，並且它在以下詳細說明。它如同在習知技術中首先包括一鍵盤 62，其管理器 620，或是根據英文術語“管理器”(“handler”)，以及一晶片卡讀卡機 7。

終端機 5 經由網際網路 RI，或是所有此種形式的網路(intranet, extranet)，而連接至遠方伺服器 4。如同在第 2 圖的情形中，它因此包括所有的邏輯與硬體元件，其允許根據在網際網路上所使用的協定，尤其是“HTTP/TCP-IP”協定而通信。因此其為無益重新描述此等元件，除非提及它包括參考號碼為 51 之“WEB”型式的領航員。此領航員 51 尤其使得能夠向伺服器 4 提出請求。它構成在終端機 5 中所出現之應用系統之一，其事實上可以包括多個。

根據本發明之第一特點，交易者應用系統之特殊應用系統是朝伺服器 4 遷移。此後者因此特別包括適當稱為 40 的伺服器“HTTP”，以及上述的客戶應用系統，其記錄在記憶體裝置 41 中。

根據本發明之另一特點，此終端機包括一第一特殊

五、發明說明 (16)

模組 50，其稱為第一通信節點或是“終端機通信節點”。此模組 50 包括傳統之通信裝置，特別是與第二圖有關所描述之協定堆疊，但是還有以下所描述的特殊元件。

根據本發明還有一個其他的特點，保全牆 6 還包括一特殊模組 60，其稱為第二通信節點，或“牆通信節點”。

此第一通信節點 50，使得網路 RI 的伺服器例如是伺服器 4 能夠通信，以及在終端機 5 之非保全部份中所存在之此等應用系統（例如是領航員“WEB”51），與在保全牆 6 中所存在的元件尤其是與晶片卡讀卡機 7 以及晶片卡 8，經由第二通信節點 60 而通信。

保全牆 6 包括一伺服器“HTTP”61，其稱為伺服器“HTTP 牆”，而設置介於第二通信節點 60 與鍵盤 62 之間。此後者構成保全牆 6 之資訊資源之一。此後者，如同它在本說明的序言中所顯示者，可以包括額外的資源 1 至 i，其在唯一獨特之參考號碼 63 下顯示。它可以例如是關於生物統計式的確認裝置，一共同處理器 (co-processor)，或是一外部翻譯器。此一個或多個資源 63，是與鍵盤 62 類似的方式，同樣地連接至伺服器“HTTP”61。

此伺服器“HTTP”61 是同樣地連接至晶片卡讀卡機 7。

此通信節點 60 使得可以導引終端機 5 的請求，經由晶片卡讀卡機 7，而朝向晶片卡 8，此在相反方向中的

五、發明說明 (17)

導引此晶片 8 之請求，經由通信節點 50，而朝向伺服器 "HTTP"61，或是朝向終端機 5。

根據本發明之一特點，伺服器 "HTTP"61 允許晶片卡 8，並且只有唯一的此卡，使用保全牆 6 的資源 62 至 63。

此不能接達鍵盤 62 或其他資源 63 的資訊，而不同的是經由扮演中間角色的晶片卡 8，是由於幾個因素：
(a)保全牆 6 是在實體上被保全（在實施上不可能“偵探”此等元件）。

(b)此節點 60 之程式是如此，它完全禁止來自外部而朝向 "HTTP 牆"61 實體的資料之通過，這是由於它位於保全牆 6 之內部；以及

(c)此 "HTTP 牆"61 實體的程式是如此，使得它不接受由晶片卡 8 之外所發出的請求，此伺服器 61 由於同樣地位於保全牆 6 之內，它同樣地受到保護。

如果(a)點本身是對於習知技術與本發明是相同，則(b)點與(c)點構成本發明特殊且有利的特點。

現在將以更詳細的方式描述經由晶片卡讀卡機 7，介於網際網路 RI 與終端機 5 之非保全部份之此等元件之間，介於這些元件與保全牆 6 之元件之間，介於保全牆 6 之此等元件之間，以及介於此等元件與晶片卡 8 之間，是如何實施通信。

根據本發明之主要特點，所有這些通信是根據一個稱為“均勻”(homogeneous)的模式而實施，其藉由使用 "URL"標準形式的位址，而同時與網際網路的協定

五、發明說明 (18)

相容，並且保存通信之標準化協定，尤其是介於晶片卡 8 與晶片卡讀卡機 7 之間(即，依據前述之 ISO 7816 準則)。

此等介於領航員 "WEB"51 與 "客戶" 伺服器 4 之間的通信不會造成特別的問題，並且可以藉由使用傳統的協定層(參閱第 2 圖)與定址 "URL"，根據 "HTTP" 協定而標準地實施。相反的如同所提到在習知技術中，它不能同樣地在介於終端機之保全元件與非保全元件之間(第 1 圖:1)，在那裡之通信通常是在 RS 232 模式中實施，也不能經由讀卡機 7，在介於保全牆 6 的這些元件與晶片卡 8 之間實施通信。在此後者的情形中，如同其參考第 2 圖所說明者，此等通信當然是藉由使用協定層而實施，但是借助於一組依據前述 ISO 7816-3 準則的指令 "APDU"而實施，因為同樣的此方式與網際網路式的協定並不相容。

同樣地，本發明建議特殊的設計使得能夠統一通信，而完全保存參與通信中元件之標準化，並且只導致較小次要的修改。

現在首先詳細說明帶給保全牆 6 與晶片卡 8 之修正，使得能夠以依據本發明的方式，以確保介於此兩個實體之間的通信。

根據本發明的特點，將晶片卡 8 配備一特殊模組其構成第三通信節點 80，以及伺服器 "HTTP"81，其以下各別稱為 "卡片通信節點"與 "卡片之伺服器 HTTP"。此在晶片卡 8 中所呈現的一個或 n 個應用系統 A₁ 至

(請先閱讀背面之注意事項再為本頁)

裝
訂
線

五、發明說明 (19)

A_n 是藉由伺服器 "HTTP" 81 的第一面而連接。藉由此等設計晶片卡 8 被轉換成對於保全牆 6 的伺服器及／或客戶 "WEB"，並且也許由位址 "URL" 而定址。

此結構的獲得是根據本發明，在基本上在晶片卡 8 中植入特殊通信之第一協定層。同樣地，一特殊通信第二協定層，其形成第一層的對稱物，是植入於保全牆 6 之中。

其中關於介於晶片卡 8 與保全牆 6 之間的交換，第 3 圖的功能示意圖可以以第 4 圖所說明的邏輯結構來代表。

在此結構中，可以重新找到習知技術之協定層，如同由第 2 圖所說明者，它扮演相同的角色，並且具有相同的參考號碼，因此無益將它們重新描述。

相反的，其雙方設有，即，在保全牆 6 中與在晶片卡 8 中，兩個額外的特殊的協定層：其各別是 64 與 84。

在保全牆 6 中，特殊層 64 是對於晶片卡 3 的協定層形成界面，即，經由多工層 13 而對底層 CC₁ 與 CC₂ 形成界面。特殊層 64 允許向晶片卡 8 傳送資料封包 (packet)。還有，它調整現存的應用系統以用於使用晶片卡 8 之應用，而不須要將它重寫。

從晶片卡 8 這邊，可以重新發現一個組織結構，其完全類似於由特殊層之額外要求所構成，此特殊層之參考號碼為 84，是層 64 之對應物。

以更正確的方式而言，這些特殊層 64 與 84，可以

(請先閱讀背面之注意事項再為本頁)

裝訂線

五、發明說明 (20)

次分成三個主要軟體元件：

— 模組 640 或 840，其經由傳統的層 CC_1 、 CC_2 、 CC'_1 與 CC'_2 ，而在此等層 13 與 23 之間傳送資訊區塊 (bloc)，

— 一或數個稱為“智慧型代理器”的軟體件 641 或 841，其例如實現協定轉換之功能，以及

— 特殊結構之管理模組 642 與 842，其類似於特殊之智慧型代理器。

因此，在保全牆 6 與晶片卡 8 中重新發現，在介於此兩個實體之間的通信協定堆疊。

此等第二位準的層（資料連接層）， CC_2 與 CC'_2 是確保介於晶片卡 8 與保全牆 6 之間的交換。這些層是負責傳送錯誤的偵測與可能更正。這些所提到不同的協定是可使用於此目的（建議 ETSI GSM 11.11；此協定是由準則 ISO 7816-3 所界定，在文字 (character) 模式 $T=0$ 中或區域模式 $T=1$ 中；或者此協定由準則 ISO 3309 所界定，在框 (frame) 模式中）。其顯示在本發明的範圍內是較佳使用在區塊模式中的協定 ISO 7816-3。

以本身所熟知的方式，在協定之每一層連接某個數目的原始軟體件，其允許在相同的位準的層之間，與從一層至另一層之資料之交換。作為例子，與第二位準層有關的原始軟體件 (primitive)，是藉由卡片之“資料請求” (“Data. request") 與“資料發送” ("Data. response")，以及“資料確認” ("Data. confirm") 等的

五、發明說明 (21)

形式。

以更特別的方式而言，這些特殊層 64 與 84 是被載入介於晶片卡 8 與主(host)，即，保全牆之間的對話中。它還允許設置一種結構其適合用於資料封包之發出及／求接收。

如同以上所顯示，這些層包括三個不同的實體。

此等第一實體模組 640 或 840 是基本上由一軟體多工器(multiplex)所構成。它允許在晶片卡 8 與終端機主(host)之間，在協定資料單元的格式下作資訊交換。它扮演與資料封包轉接器(commuter)類似的角色。此等單元是經由第 2 位準層(資料連接層)而發射或接收。此通信特殊協定至少允許一對"智慧型代理器"之通信。每一對之第一代理器 641，是位於保全牆 6 這邊的層 64 之中，此第二代理器 841 是位於晶片卡 8 這邊之層 84 之中。兩個"智慧型代理器"之間的連接是與一會議有關。一個會議是介於兩個代理器之間之雙向資料交換。

智慧型代理器根據保全牆 6 所使用的結構，可以實現第三與第四位準層之全部或部份的功能。

一特殊之智慧型代理器是藉由例如在 16 位元(數目包括介於 0 與 6535 之間)上之整數而有利地辨識。此辨識器被使用於例如構成來源參考號碼與目的地參考號碼之協定資料單元之中。

此存在兩大種類的智慧型代理器："伺服器"型式的代理器，其由固定的參考號碼所辨識，以及"客戶"

(請先閱讀背面之注意事項再為本頁)

裝

訂

線

五、發明說明 (>>)

型式的代理器，其由可變的參考號碼所辨識，此等號碼是由結構管理模組 642 或 842 所發給。

此會議開啓的方法通常如下：“客戶”(client)型式的智慧型代理器朝向“伺服器”型式的智慧型代理器開啓此項會議。模組 642 與 842 管理此表(未圖示)，其包括終端機 6 與晶片卡 8 這邊之所存在的智慧型代理器之列表。

這些智慧型代理器 641 或 841 是與特殊的特性或屬性有關。爲了確定此等概念並且作爲非窮盡的例子，智慧型代理器與以下的四個特性有關：

- “主”：位於保全牆中的代理器；
- “卡片”：位於卡片中的代理器；
- “客戶”：開啓會議之代理器；
- “伺服器”：接收開會要求之代理器。

此等智慧型代理器允許資料之交換。

此等結構管理模組 642 與 842，如其顯示各自分別類似於特殊智慧型代理器。例如在終端機 6 這邊的模組 642，是特別管理有關於保全牆 6(功能模式)的結構，其他所存在代理器之列表，等等，在晶片卡 8 這邊的模組 842，具有類似的功能。此兩個代理器可以彼此通信以建立會議。

根據本發明的一特點，晶片卡 8 向系統主(host)，即，向保全牆 6 建議一虛擬終端機型式。爲了如此做，晶片卡 8 表現如同伺服器及／或客戶“WEB”。

以實際的方式，晶片卡 8 是藉由使用位址“URL”而

五、發明說明 (3)

有利地 " 定址 "，此位址在經由終端機 5 並且更特別地是在經由保全牆 6 界定一經由迴路迴歸 (loop back) 且在例如是伺服器 4 的外部伺服器上沒有作記號。作為例子，此 "URL" 的結構通常如下：

http://127.0.0.1:8080 (1) 或

http://local host:8080 (1 至)

在其中 127.0.0.1 是經由迴路迴歸 (loop back) 之 "IP" 之位址 ("local host" 是 127.0.0.1 之字義翻譯)，並且 8080 是埠口的號碼。資源 62 及 / 或 63 之位址 "URL" 是可以藉由 "/xxx" 型式之後綴詞 (suffix) 而完成。例如，鍵盤 62 之管理模組 620 可以具有如同以下之位址 "URL"：

http://local host:8080/kb (2)

此邏輯結構允許介於適當稱為終端機 5 (介於節點 50 與 60 之間)，即，此終端機之未保全元件與保全牆 6 之間的通信，其類似於在第 4 圖上所顯示者。因此，此會議可以依照剛才所描述的一般性的示意圖，而在通信節點 50 與 60 之間建立。保全牆是特別可以藉由位址 "URL" 而被定址，此位址是與晶片卡的埠口相同的號碼，或是在所說明的例子中的 8080。

此通信節點 50 還允許終端機 5 與網際網路 RI 通信。同樣地，除了與以上所列舉之智慧型代理器有關的特性外，它同樣地存在以下的兩個特性：

- " 區域性 "：不與網路通信的代理器；
- " 網路 "：與網路通信的代理器。

五、發明說明 (24)

整個的終端機 5 是由與以上相同的位址 "IP" 而定址。它容納至少一個稱為終端機的應用系統，其有利的是領航員 "WEB" 51。其與特殊的埠口有關。

作為例子，藉由網頁 "WEB" 與超連接 (hyperlien) 的技術，使用者 (未圖示) 可以在可供自由使用的物件中選擇一項產品或服務，並將此請求傳送給客戶伺服器 4。

除了由晶片卡 8 所提供之 "WEB" 主-從式 (serveur-client) 功能外，根據本發明之一特點，它包括在其中一個類似於稱為 "CGI" (代表 "共同閘道界面" "Common Gateway Interface") 功能之機構，其植入於傳統式的伺服器 "WEB" 中。

在描述依據本發明的構造例子，其允許實現晶片卡 8 之內部本身之型式的功能之前，其為有益回憶 "CGI" 功能模式的主要特點。

此 "CGI" 是一種規格其使用以從伺服器 "WEB"，撰寫應用系統而用於執行系統 "UNIX" (標記設置)、"DOS" 或 "WINDOWS" (標記設置)。作為例子，用於執行系統 "UNIX"，其規格是 "CGI 1.1"，以及用於執行系統 "WINDOWS 95"，其規格是 "CGI 1.3"。

總是作為例子，一個對於位址 "URL" 的請求 "HTTP" 是此種形式：

"http://www.host.com/cgi-bin/xxx" (3)，

在其中 "host" 是提到一主 (host) 系統 (通常是遠方)，其由伺服器 "WEB" 解釋如同執行一命令劇本，其形式

(請先閱讀背面之注意事項再為本頁)

裝

訂

線

五、發明說明 (25)

爲 "CGI" 名稱爲 "xxx" 並且呈現於主系統之目錄 "cgi-bin" 中。雖然，此目錄的名稱先天的爲任何名稱，由慣例此給予目錄的名稱是儲存 "CG" 型式的劇本。一個劇本是主 (host) 系統之執行系統之一組指令，其最後的結果被傳送至領航員 "WEB" 其發出上述的請求，或是傳送至所有其他的應用系統其要求此項服務，如同交易者伺服器。不同的語言可以被使用，以撰寫此劇本，例如是 "PERL" 語言 (標記設置)。

在實際的方式，此項請求通常是顯示於，包括在網頁 "HTML" 中之表格形式下之資訊螢幕上。此語言 "HTML" 允許在位址 "URL" 設置一表格。此表格包括一或數個強制性或非強制性的欄位，其由使用者借助於一般的擷取裝置填入：對於文字是用鍵盤，對於作記號是用滑鼠，或是用稱爲 "radio" 之按鈕，等等。此表格之內容 (以及可能稱爲 "隱藏" ("cachées") 之資訊與指令) 是發出至伺服器 "WEB" 之目的地。此網頁的 "HTML" 碼是描述此表格的硬體結構 (範圍、圖形、顏色、以及所有其他的屬性)，以及所擷取資料欄位之結構 (名稱、長度、資料之形式，等)。

此傳送可以根據主要 "HTTP" 格式之兩個形式而執行。第一格式使用稱爲 "POST" 之方法，並且第二格式使用稱爲 "GET" 的方法。此格式形式的資訊是存在於網頁表格之碼之中。

然而此機構並不可直接地傳送給晶片卡，即使它提供依據本發明特點之一的伺服器 "WEB" 之功能。

(請先閱讀背面之注意事項再為本頁)

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 (> 6)

現在參考第 5 圖以說明一結構的例子，其使得能夠經由在晶片卡上的伺服器 "WEB"，以傳統的形式啟動任何一個應用系統。

客戶伺服器 4 啟動一在位址 "URL" 之 "GET" 形式之請求 "HTTP"，其可以以下列的方式呈現：

http://@carte:8080/xxx.8080/cgi-bin/le-cgi?

param1+param2 (4)，

在其中 "@carte" 是終端機的位址 "IP"，其容納晶片卡（例如關係式 (1) 之經由迴路迴歸 (loop back) 之位址 "127.0.0.1"），"le-cgi" 是在晶片卡 8 上之所執行之特殊據本 "CGI"，以及 "param1" 與 "param2" 是進入上述劇本之參數。此請求是經由通信節點 50 與 60 而首先傳送至保全牆 6（第 3 圖）。

一個會議是建立於終端機與晶片卡讀卡機之間。然後另一個會議是建立於一對智慧型代理器 641 與 841 之間，其分別位於保全牆 6 的特殊層 64 之中，與晶片卡 8 之特殊層 84 之中。這些資料，經由特殊通信協定層 64 之封包多路轉換器 (multiplexer) 640。它們然後經由傳統之協定層（參閱第 2 圖）。然而，為了更佳的證明本發明之某些特殊的觀點，以下將作說明，在第 5 圖上此等層被設計成兩部份：指令管理器 "APDU" 65a 與底部協定層 65b（準則 ISO 7816-3）。

同樣的，在晶片卡 8 之中，此等資料經由參考號碼為 85b 的底部協定層，與參考號碼為 85a 之卡片這邊的指令管理器 "APDU"，然後經由封包之多路轉換器

(請先閱讀背面之注意事項再為本頁)

裝 · 訂 · 線

五、發明說明 (7)

840，而由智慧型代理器 841 接收，其稱為“代理器 WEB”。

其為合適地指出，此等定址於代理器“WEB”841 的資料是可以本身習知的方式，在用於“封包多路轉換器”840 之特殊應用系統，在指令“APDU”的格式下被傳送。此指令管理器“APDU”85a，以完全類似於選擇出現在晶片卡 8 中其他的應用系統 A₁ 至 A_n 的方式，而選擇此應用系統。換句話說，此封包之多路轉換器 840 被指令管理器“APDU”85a 視為如同一平常之卡片應用系統。

此請求“HTTP”被代理器“WEB”841 分析，其偵測並提到一特殊目錄，而一方面以下由於慣例稱為“cgi-smart”，並且提到一特殊之應用系統，例如是 A_i。此完整的行程因此在這種情況下是“cgi-smart/A_i”。

根據本發明之方法之一特點，以上的實體設計一特殊的劇本，其與同樣特殊的應用系統有關。

根據本發明之一特點，在晶片卡 8 中插特殊智慧型代理器，其以下稱為“劇本之翻譯代理器”，或者以字母縮減的方式稱為“ATS”。此劇本被一智慧型代理器所解釋。此翻譯可以以不同的方式實現：

- (a)由代理器“WEB”841 本身，其在此情況中配備了雙倍的容量；
- (b)由一唯一的劇本代理器，其能夠翻譯在晶片卡 8 中所出現的整個劇本；
- (c)由一專用的劇本代理器，其以下稱為“ATSD”，或

五、發明說明 (28)

(d)由指令管理器 "APDU"85a 之代理器 "APDU"850a，
其在此情況中，配備了雙倍容量。

代理器 "APDU"850a 是指令管理器層 "APDU"85a 的
構成部份。此後者是一層能夠將所有由此系統所發出
及／或接收的指令 "APDU"集中，存 A_1 至 A_n 中選擇應
用系統，但同樣地提供智慧型代理器型式的界面。它
因此能夠根據本發明的特點之一，與所有的智慧型代
理器（經由會議）而通信，不論此等代理器是位於保
全牆 6 或晶片卡 8 之中。

在以上(c)的情況之中，是在代理器 "WEB"841 與代
理器 "ATSD"之一之間開啓一會議。

第 5 圖說明一結構之例子對於它此等翻譯代理器是
"ATSD"型式。它們是以 ATS_1 至 ATS_n 表示，並且與應
用系統 A_1 至 A_n 有關。若所選擇的應用系統假設是應
用系統 A_i ，則在代理器 "WEB"841 與代理器 ATS_i 之間
建立會議。

一劇本翻譯代理器管理一組 "APDU"指令。一會議是
開啓介於例如是代理器 ATS_i 之翻譯代理器與代理器
"APDU"850a 之間。然而，此等指令是朝 "APDU"850a
代理器發出。指令管理器 "APDU"85a 選擇應用系統
"CGA" A_i ，並且向它傳送指令 "APDU"，此指令是被翻
譯並且因此是協定的，所以它能夠瞭解。此應用系統
因此被正確的啓動，而不需要修改或重寫。

應用系統 A_i 的回應被傳送至指令管理者 "APDU"
85a，至代理器 "APDU"850a，然後重新至 ATS_i 代理器

五、發明說明 (9)

(以及更一般的方式至劇本翻譯代理器)。

這些不同的逐漸發展是在第 5 圖上藉由連接這些功能塊的實線，或是在這些功能塊中的虛線以符號的方式來表示。

爲了確定此等概念，而沒有限定本發明的範圍，此定址之技術今後是在其一般性中界定，現在以下將詳細說明各種可能的路徑，其稱爲實施例，並且以 CU-n 代表：

CU-1: 介於交易者伺服器 4 與晶片卡 8 之間的通信。

爲了如此作，而使用依據式(1)的位址 "URL"。在此情況中，不須要使用鍵盤 62。此項請求，經由網際網路 RI 傳送，而抵達通信節點 50 上。它辨識與晶片卡有關的埠口，即，埠口 8080，它與保全牆 6 之埠口相同。通信節點 50 向通信節點 60 發送此項請求。在所有的情形中，不論是那一個位址 "URL"，通信節點 60 將所接收的資料封包朝晶片卡 8 發送，並且更正確地說是經由通信節點 80，向晶片卡 81 之伺服器 "HTTP" 發送。最後，它啓動晶片卡 8 的應用系統之一，例如是應用系統 A₁。

CU-2: 晶片卡 8 的兩個應用系統之間的通信。

例如，應用系統 A₁ 想要與應用系統 A_n 通信。由應用系統 A₁ 所發出的請求是藉由伺服器 "HTTP" 81 而發送。以實際的方式而言，此會議是根據參考第 4 圖中所說明的示意圖，而在位於晶片卡 8 中的一對智慧型代理器之間建立。通信節點 80 沒有參與加入，它沒有

(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)

調整所設的通信協定。

CU-3：介於應用系統卡片與伺服器 4 中客戶應用系統 41 之間的通信。

此種情況之產生尤其是當晶片卡 8 收到客戶伺服器 4 的請求 (CU-1 之例)。晶片卡 8 的一個局部應用系統，例如是應用系統 A₁ 可以被啟動。一個由所接收之請求所控制之特定動作是在晶片卡的內部實現，其例如是 "CGI" 型式的動作，藉由執行劇本或是所有相等的方法而實現。此動作是在劇本之翻譯智慧型代理器的控制下實現，如同它參考第 5 圖所說明者。

其結果是應用系統 A₁ 提出一請求，其以伺服器 4 為目的。在檢驗其位址 "IP" 後，伺服器 "HTTP" 81 將此請求朝向通信節點 80。它在晶片卡 8 與保全牆 6 之間建立會議，而更正確的說，是根據參考第 4 圖所說明的示意圖，在通信節點 60 與 80 之間建立會議。同樣地，通信節點 60，在檢驗位址 "IP" 之後，將此請求傳送給通信節點 50。它在檢驗位址 "IP" 之後，輪到它經由網際網路 RI，朝它最後的目的地，即，朝向伺服器 4 傳送此請求。

此過程在此交易時間可以在晶片卡 8 與伺服器 4 之間包括數個來回。當此過程結束 (例如在 "CGI" 的結束)，此晶片卡的回覆，特別是經由相繼連續的通信節點 80、60 與 50，而傳送給交易者伺服器 4。

CU-4：介於 " 應用卡 " 與 " 應用終端機 " 之間的通信。

(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
為本頁)

裝
訂
線

五、發明說明 (31)

作為例子：應用系統 A_i 例如欲與終端機之塗層 (impression) 管理器 (未圖示) 通信，並且在此方向提出請求。在檢查了位址 "IP" 與埠口號碼之後，伺服器。"HTTP" 81 將此請求朝向通信節點 80。此項請求然後跟隨著在 CU-3 例子中相同的路徑，一直到它到達通信節點 50。此節結 50，在檢查位址 "IP" 與埠口號碼之後，將此請求朝向終端機應用系統位址，例如是塗層管理器位址。

CU-5：在 " 卡片應用系統 " 與保全牆資源之間的通信。

首先假設，在此實施例中，晶片卡 8 是在相對交易者伺服器 4 之 "slave" 模式中，並且此伺服器向晶片卡 8 的目的地發出請求。此請求被在 CU-1 與 CU-3 的例子所說明的方式處理。它以參考第 5 圖所描述的方式，執行例如在晶片卡 8 內部的 "CGI 交易者"。此劇本藉助於劇本翻譯代理器之例如是 ATS_i ，而執行啟動例如是 A_i 之應用系統之一。假設 CGI 交易者須要來自鍵盤 62 之資訊 (例如 " 口令 " " pass word ")，或是其他的確認資訊 (來自構成資源 63 之一的生物統計裝置)。此在討論中的 CGI 應該以一特殊位址 "URL" 來執行。應用系統 A_i 發出一請求，其位址是例如由以上式 (2) 所提供。此後綴詞 "/kb" 的出現顯示通信節點 60，其應該將此請求回歸朝向伺服器 "HTTP" 61，而輪到它來啟動鍵盤 62 之管理器 620，並且收回所期待的資訊 (例如擷取一口令 "pass word")。此項請求的回覆藉

經濟部智慧財產局員工消費合作社印製

五、發明說明 (32)

由相同的途徑但以相反的方向朝向晶片卡 8 傳送。

交易者伺服器 4 的請求之回覆被傳送回此伺服器。
在許多時候，此對話可以以類似於 CU-3 例子的方式建立。

在一交易 (transaction) 時間的期間可以執行數個 CGI。

爲了確定此等概念，第一個 " CGI 交易者 " 可以具有結果，其顯示於包括在保全牆 6 中的螢幕上 (在唯一的參考號碼 63 下所代表的資源之一)，其訊息邀請使用者撰寫一碼並且顯示其總額。第二 CGI 讀取例如由鍵盤 62 所傳送之資訊。第三 CGI 可以具有 "CODE CORRECT" 型式之訊息或是所有類似訊息在相同視覺裝置上的結果。

CU-6：介於終端機與保全牆資源之間的通信。

作爲例子，終端機 5 之應用系統 (在其非保全的部份中)，例如是領航員 "WEB"51，想要與保全資源之一例如是與鍵盤 62 通信，並且朝此方向發出請求。通信節點 60 檢查 "URL" 位址，辨認此保全牆 6 之埠口號碼，並且將此請求傳送給此牆。此通信節點 60，由於其程式，有系統地將所收到的請求，即使它的目的是保全牆內部資源之一，導向晶片卡 8。根據其階段，此請求是跟隨著類似 CU-1 例子的途徑。此由晶片卡 8 決定是否將此請求傳送回原先定址之保全資源，並可能將它修改。此決定可能的結果是一辨認程序參與檢查在晶片卡中所記錄之保全資料，尤其是在唯讀型式

(請先閱讀背面之注意事項再
為本頁)

裝
訂
線

五、發明說明 (33)

記憶體中，並可能是在編碼的形式下。如同在例子 CU-4 中，在保全牆 6 外的元件因此是不能直接對保全資源接達存取。

此最後之特性允許更新在保全牆 6 中的常駐軟體，以較在習知技術中更安全可靠的方式，至少部份地附加於此軟體或將其刪除。事實上，這是根據儲存在保全牆 6 軟體中的鑰匙，而使用此種性質修正之確認。

由於只有晶片卡 8 可以由外部對於保全牆 6 所保護的資源接達存取，此軟體資源之電傳下載因此可以由網際網路伺服器借助晶片卡而實施，並完全保存非常大的安全程度。此電傳下載的資料如果是敏感的話，只須使用一堅實的算式(algorithm)及／或足夠長的編碼鎖將其適當地編碼。由於晶片卡 8 之中間功能的角色，在本發明中所使用的機構，較僅只將鑰匙儲存於保全牆 6 之記憶裝置（未圖示）中更為強而有力。

吾人同樣地可以將記錄在晶片卡 8 中的軟體件電傳下載，而從晶片卡 8 直接修改保全牆 6 之軟體資源之內容。然而，如此電傳下載的軟體容量是受限於晶片卡（記憶體容量）本身的資源，這不是一開始的情況從伺服器"WEB"經由網際網路而電傳下載此伺服器可以提供重要的資訊資源。此電傳下載的時間是自然取決於所下載軟體的數量。但使用高速的數據機及／或高流量的通信線，自然將用於所考慮之應用系統的時間完全保持在合理極限之中。

在閱讀了以上的說明之後，可以容易地察覺確實達

（請先閱讀背面之注意事項再
寫本頁）

裝

訂

線

五、發明說明 (34)

成它所設之目標。

它尤其允許完全保存此可能性而使用傳統的組成成份以及正規的通信模式，尤其是經由讀卡機而介於保全牆與晶片卡之間的通信，一位址以及與網際網路協定 "HTTP" 相容的通信。它將晶片卡轉變成主一從 "WEB"，能夠執行 "CGI" 型式的作業。它尤其允許經由網際網路從伺服器 "WEB"，或是在相反的方向，直接定址並且與晶片卡互相作用，它不須要在終端機本身上與保全牆上任何特殊的客戶應用系統。它提供一非常大的靈活性並且容易地適用於各種應用領域。它只造成所使用組成成份次要的修正，此等修正主要歸結於植入特殊的軟體件，並必須理解，"特殊" 這字並不表示對於所處理應用系統之依賴。尤其在晶片卡中的常駐 (resident) 應用系統保持應用系統的標準，並且不須要重寫。還有此等特殊應用系統從 "交易者應用系統" 的觀點是完全位於遠方伺服器 "WEB" 之中。此伺服器可以包含多個特殊應用系統。此等應用系統之更新、刪除、以及增加新的應用系統是很容易的事情。此特點提供很大的彈性。此連接於伺服器上的所有的終端機的程式的版本是相同。最後，本發明所保障的安全是非常的大。其用於網際網路上的通信可以要求結實的編碼算法以及很大長度的鎖。還有，根據本發明的特點，所有來自保全牆之外的請求，不論是從終端機非保全的部份或是直接從網際網路，應該強制性的經由晶片卡，並且保持在它唯一的控制之下。此晶

(請先閱讀背面之注意事項再
為本頁)

裝
訂
線

五、發明說明 (35)

片卡根據例如常駐的保全資料單獨地決定應該作此等請求的決定。然而，晶片卡的持有者保持其所有權。

然而其應為明顯，本發明並不受限於所明確說明僅的實施例，尤其是有關於第 3 至 5 圖。

在一實施模式（未圖示）中，保全牆可以只包含一個晶片卡讀卡機，此等記錄在晶片卡中的應用系統本身足夠用於持有者的確認及／或允許晶片卡與遠方伺服器"WEB"之間的交易。此鍵盤可以被省略並且由保全資源之一例如是生物統計裝置取代。最後，可以在第一晶片卡讀卡機上增設第二甚至數個晶片卡讀卡機。

符號說明

- 1… 終端機
- 2… 晶片卡
- 3… 保全牆
- 4… 伺服器"WEB"
- 5… 終端機
- 6… 保全牆
- 7… 晶片卡讀卡機
- 8… 晶片卡
- 10… 特殊應用系統
- 11… 接達電路
- 13… 層
- 14… 網路程序集
- 15… 底層驅動器

(請先閱讀背面之注意事項再寫本頁)

裝
訂
線

五、發明說明 (36)

- 23… 層
- 30… 讀卡機
- 31… 鍵盤
- 50… 第一通信節點
- 51… 領航員 "WEB"
- 60… 第二通信節點
- 61… 伺服器 "HTTP"
- 62… 鍵盤
- 63… 其他資訊資源
- 64… 特殊協定層
- 81… 伺服器 "HTTP"
- 84… 特殊協定層
- 640… 模組
- 641… 智慧型代理器
- 642… 管理模組
- 840… 模組
- 841… 智慧型代理器
- 842… 管理模組
- C₁… 層 1
- C₂… 層 2
- C₃… 層 3
- C₄… 層 4
- CC₁… 層 1
- CC₂… 層 2
- RI… 網際網路

(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： 經由網際網路式網路而與伺服器
通信所用之配備有晶片卡讀卡機
之保全終端機)

本發明是有關一種終端機(5)結構，其使得晶片卡(8)與伺服器"WEB"(4)之間能夠經由網際網路式之網路(RI)而通信。此終端機(5)配備了保全牆(6)，其包括一晶片卡讀卡機(8)，一鍵盤(62)，以及以選擇的方式，其他的資訊資源(63)。此終端機(5)之非保全部份包括領航員"WEB"(51)與第一通信節點(50)，將所收到的請求導引向領航員(51)或保全牆(6)。保全牆(6)包括第二通信節點(60)與伺服器"HTTP"(61)。晶片卡(8)包括第三通信節點(80)與伺服器"HTTP"(81)。伺服器"WEB"(4)包括一交易者應用系統(41)可以與晶片卡(8)通信，並且啟動晶片卡的軟體應用系統(A₁-A_n)。

(請先閱讀背面之注意事項再填寫本頁各欄)

裝

訂

線

四、~~英~~文發明摘要 (發明之名稱: Security terminal equipped with a chip) card reader used for communication with a server via the Internet type network

This invention relates to a terminal (5) architecture which permits the communication between a chip card (8) and a server “WEB” (4), via an Internet (RI) type network. The terminal (5) is equipped with a security wall (6) containing a chip card (8) reader, a keyboard (62), and in an optional fashion, other information resources (63). The non-security portion of the terminal (5) comprising a navigator “WEB” (51) and a first communication node (50) switching the request received to the navigator (51) or to the security wall (6). The security wall (6) consists of a second communication node (60) and a server “HTTP” (61). The chip cards (8) comprises a third communication node (80) and a server “HTTP” (81). The server “WEB” (4) comprises a transaction application (41) which can communicate with the chip card (8) and activate its application software (A1-An).

(請先閱讀背面之注意事項再填寫)

裝

訂

線

修正
91. 9. 17 年 月 日 補充

六、申請專利範圍

第 89122702 號「經由網際網路式網路而與伺服器通信所用之配備有晶片卡讀卡機之保全終端機」專利案

(91 年 9 月 17 日修正)

六 申請專利範圍：

1. 一種配備了保全牆之終端機，其用於根據網際網路型式的第一通信協定，經由網際網路型式的網路，而與至少一"WEB"型式的伺服器通信，該保全牆包括至少一個晶片卡讀卡機，該晶片卡至少儲存一軟體應用系統，其特徵為：

該終端機(5)包括一非保全部份，其包括至少一稱為第一通信節點(50)的第一模組，該保全牆(6)包括至少一稱為第二通信節點(60)的第二模組，並且該晶片卡(8)包括至少一稱為第三通信節點(80)之第三模組，其中該等通信節點(50,60,80)各自包括第一、第二與第三協定堆疊，其各包括稱為標準以及第一、第二與第三特殊軟體件(64,84)的通信軟體層，其各自包括至少一第一軟體實體(641,841)，該等第一軟體實體是兩個兩個配成對，其中該第一節點(50)允許至少根據網際網路式的該第一通信協定，而介於該終端機(5)與該伺服器"WEB"(4)之間

修正
年 月 日
91. 9. 17 補充

六、申請專利範圍

的通信，其中該第一與第二特殊軟體件之該第一實體，允許根據所確定之第二通信協定，在該終端機(5)與該保全牆(6)之間建立資料雙向交換會議，其中該第二(64)與第三(84)特殊軟體件之該第一實體(641,841)，允許至少經由該晶片卡讀卡機，根據所確定之第三通信協定，在該保全牆(6)與該晶片卡(8)之間建立資料雙向交換會議，以便在該"WEB"型式的伺服器(4)與晶片卡(8)之該等軟體應用系統(A_1-A_n)之至少一個之間建立關係。

2. 如申請專利範圍第1項之終端機，其中該第一對實體是由稱為智慧型代理器(641,841)的軟體模組所構成，其建立該等會議。
3. 如申請專利範圍第1項之終端機，其中它在其非保全的部份中包括，至少一個由"WEB"型式的領航員(51)所構成的應用系統，其中該網際網路式的第一協定是"HTTP/TCP-IP"協定，其包括一稱為"URL"型式的位址，其包括一個稱為"IP"的網際網路位址元件與一埠口號碼，用以選擇該終端機(5)與此終端機(5)之內部元件，其中該第一通信節點(50)之該特殊軟體件之該

六、申請專利範圍

第一實體鑒定該位址元件 "IP" 與該埠口號碼，其中，該鑒定的結果是，此等從該 "WEB" 型式的伺服器 (4) 所接收的資料，根據該網際網路式的第一協定，而被導引向該 "WEB" 型式的領航員 (51)，或者將它翻譯並且根據所確定之該第二通信協定，而在資料第一傳送方向中向該第二通信節點 (60) 傳送，並且其中經由該鑒定，此由第二通信節點 (60) 所接收的資料，被導引朝向該 "WEB" 型式的領航員 (51)，或是根據該網際網路式的第一通信協定，在資料傳送的第二方向中導向該 "WEB" 型式的伺服器 (4)。

4. 如申請專利範圍第 3 項之終端機，其中該保全牆 (6) 還包括至少一資料擷取鍵盤 (62)，以及設置介於該鍵盤 (62) 與該第二通信節點 (60) 之間稱為牆 (61) 的至少一伺服器 "HTTP"，其中該第二通信節點 (60) 之該特殊軟體件 (64) 之該第一實體 (641) 鑒定該位址元件 "IP" 與該埠口號碼，其中此等從第一通信節點 (50) 所接收的資料被翻譯，並且總是根據所確定之第三通信協定，而在資料傳送之第一方向中，將它朝向該第三通信節點 (80) 傳送，並且經由鑒定，此等

六、申請專利範圍

從第三通信節點(80)所接收的資料被導引朝向該伺服器"HTTP"(61)，或者根據所確定之第二通信協定，在資料傳送的第二方向中，將其朝向該第一通信節點(50)傳送。

5. 如申請專利範圍第4項之終端機，其中該保全牆包括至少一個連接至該保全牆(6)之伺服器"HTTP"(61)的額外資訊資源(63)，並且其中該"URL"式的位址包括一額外元件，該伺服器"HTTP"(61)，經由鑒定(identify)該額外位址元件，而選擇該鍵盤(62)或該等額外資訊資源(63)之一。
6. 如申請專利範圍第5項之終端機，其中該額外資訊資源(63)是生物統計鑒定裝置。
7. 如申請專利範圍第4項之終端機，其中該晶片卡儲存數個軟體應用系統($A_1 - A_n$)，其中它包括設置介於該軟體應用系統($A_1 - A_n$)與該第三通信節點(80)之間的稱為卡片(81)的伺服器"HTTP"，經由接收來自該第二通信節點(60)之請求，而選擇性地啟動該等軟體應用系統($A_1 - A_n$)至少之一，或者將由該等應用系統($A_1 - A_n$)所發出的請求，朝向該第三通信節點(80)傳送。

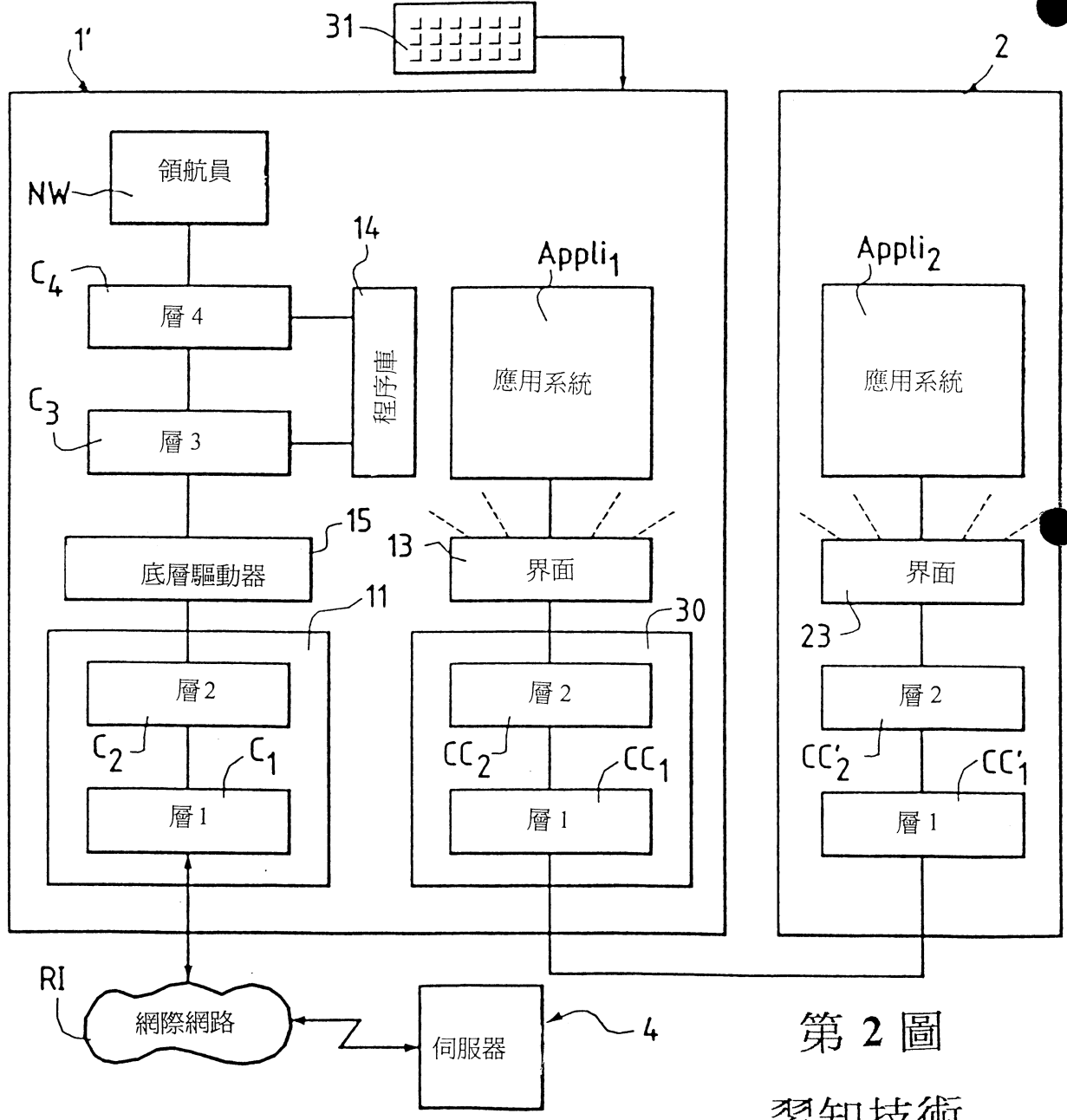
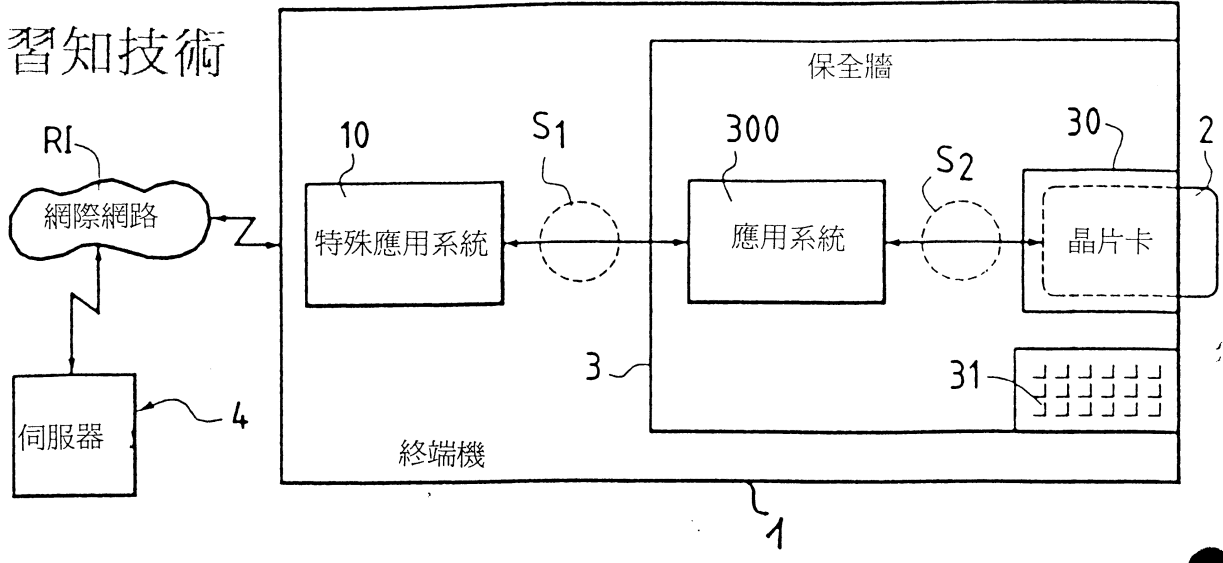
修正
91. 9. 17 補充

六、申請專利範圍

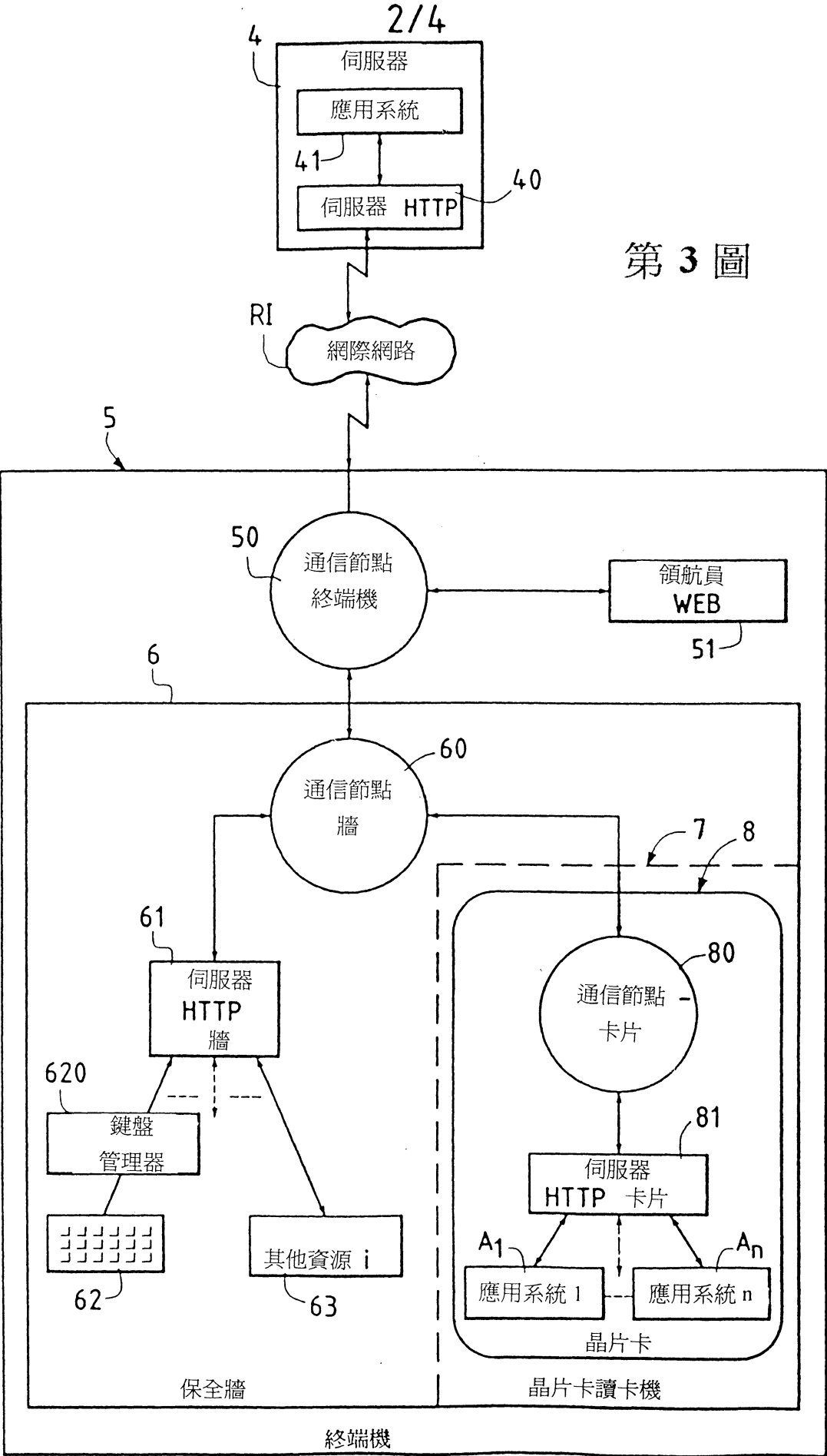
8. 如申請專利範圍第 7 項之終端機，其中該晶片卡(8)還包括一第二軟體實體(ATS_1-ATS_n)，其適用於說明解釋其所接收來自第三通信節點(80)而由該等資料所傳送的一組命令(instruction)，並且將它翻譯成一組指令(order)，該等第二軟體實體(ATS_1-ATS_n)與該等軟體應用系統(A_1-A_n)以及該第三通信節點(80)之該特殊軟體件(84)合作作業，該組被翻譯的命令與該等軟體應用系統配合，以啟動該晶片卡(8)之(A_1-A_n)。
9. 如申請專利範圍第 8 項之終端機，其中該組翻譯用之命令是由一劇本(script)所構成，各個該第二軟體實體是由稱為智慧型劇本翻譯代理器(ATS_1-ATS_i)的軟體模組所構成。
10. 如申請專利範圍第 1 項之終端機，其中該"WEB"式的伺服器(40)儲存稱為交易者(41)之軟體應用系統，其用於經由該第一(50)、第二(60)與第三(80)通信節點，與晶片卡(8)之該等軟體應用系統(A_1-A_n)之至少一作對談式(interactive)的通信。

第 1 圖
習知技術

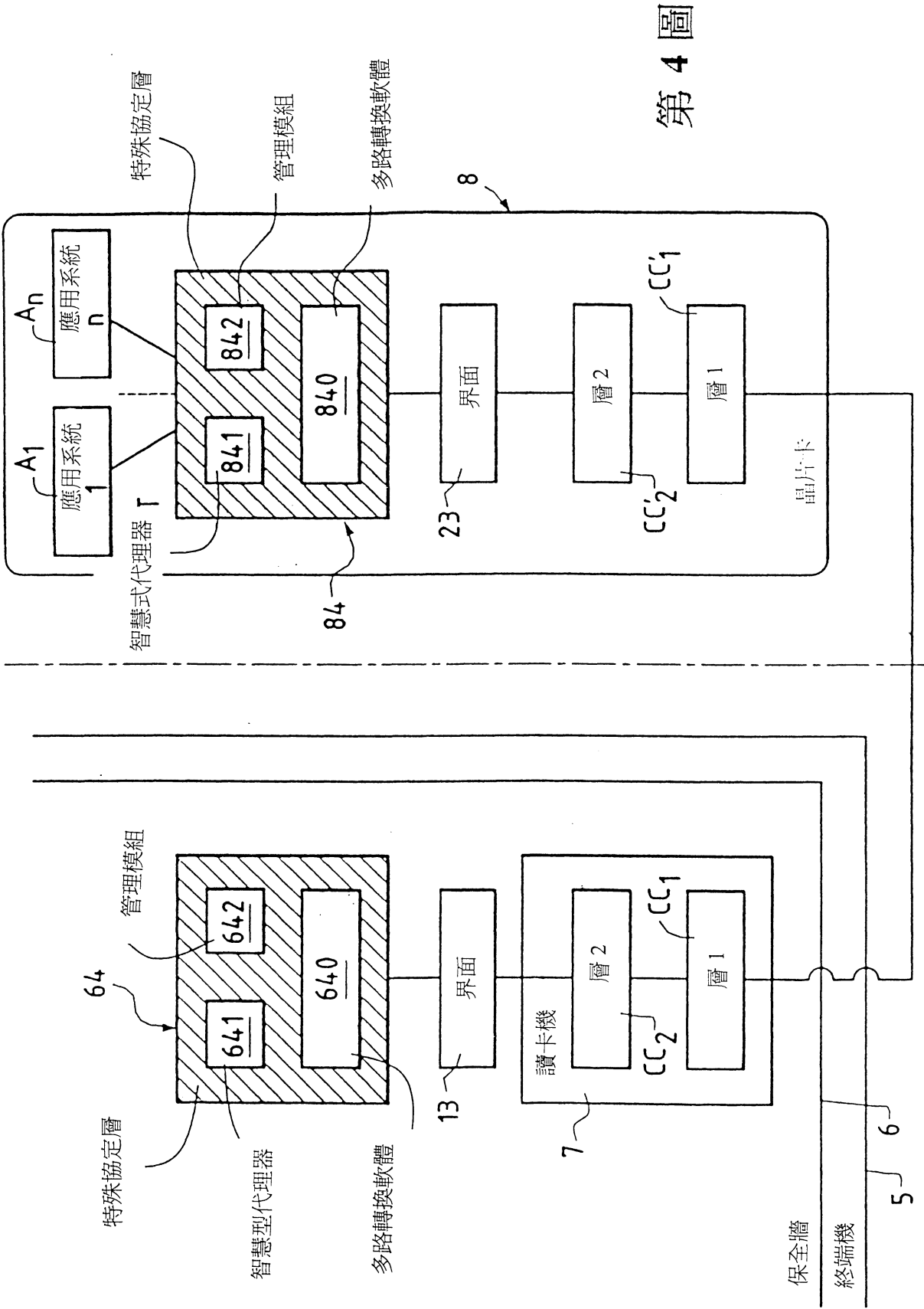
1/4



第 2 圖
習知技術



第 3 圖



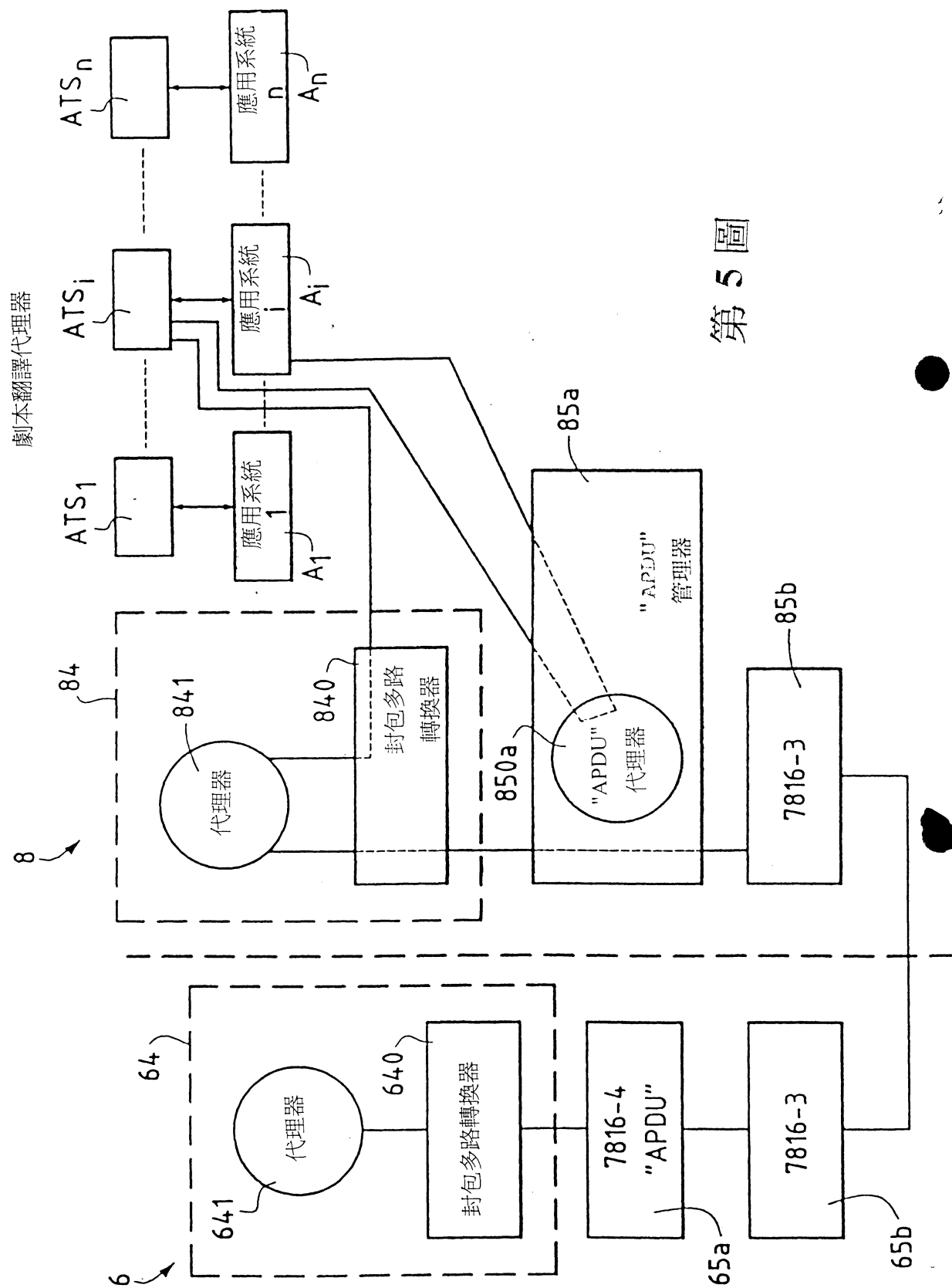


圖
5
架