# 發明專利說明書

公告本

（本說明書格式、順序及粗體字，請勿任意更動，※記號部分請勿填寫）

※ 申請案號：97142292

※ 申請日期：97.10.31　　※IPC 分類：~~G06F~~ G06K 19/07 (2006.01)
G06K 19/00 (2006.01)

一、發明名稱：（中文/英文）

基於行動智慧卡之鑑認

MOBILE SMARTCARD BASED AUTHENTICATION

二、申 請 人：（共 1 人）

姓名或名稱：（中文/英文）

美商萬國商業機器公司
INTERNATIONAL BUSINESS MACHINES CORPORATION

代表人：（中文/英文）

琳恩 D 安德森
ANDERSON, LYNNE D.

住居所或營業所地址：（中文/英文）

美國紐約州阿蒙市新果園路
NEW ORCHARD ROAD, ARMONK, NY 10504, U.S.A.

國 籍：（中文/英文）

美國 U.S.A.

三、發明人：（共 1 人）

姓 名：（中文/英文）

包瑞斯 巴瑟
BALTZER, BORIS

國 籍：（中文/英文）

德國 GERMANY

## 四、聲明事項：

☐ 主張專利法第二十二條第二項☐第一款或☐第二款規定之事實，其事實發生日期為：　年　月　日。

☑ 申請前已向下列國家（地區）申請專利：

【格式請依：受理國家（地區）、申請日、申請案號　順序註記】

☑ 有主張專利法第二十七條第一項國際優先權：

1. 歐洲專利機構；2007年12月07日；07122616.1

2.

☐ 無主張專利法第二十七條第一項國際優先權：

1.

2.

☐ 主張專利法第二十九條第一項國內優先權：

【格式請依：申請日、申請案號　順序註記】

☐ 主張專利法第三十條生物材料：

☐ 須寄存生物材料者：

國內生物材料 【格式請依：寄存機構、日期、號碼　順序註記】

國外生物材料 【格式請依：寄存國家、機構、日期、號碼　順序註記】

☐ 不須寄存生物材料者：

所屬技術領域中具有通常知識者易於獲得時，不須寄存。

## 五、中文發明摘要：

在一鑑認伺服器中，在鑑認準備階段期間接收表示對一查問之一回應之一第一部分的資訊。儲存該查問及該回應之該第一部分以用於進一步使用。在一經修改鑑認階段期間重新發送該查問且接收表示對該查問之該回應之一第二部分的資訊。對照該查問來檢查該回應之該第一部分及該第二部分以用於鑑認使用者。在一智慧卡讀取器中，當該智慧卡讀取器在正常鑑認期間經由至一計算設備之一介面而接收到該查問時，將自智慧卡所接收之該回應發送至該計算設備。回應於該智慧卡讀取器已在一鑑認準備階段期間經由至該計算設備之該介面而接收到該查問，該智慧卡讀取器將該回應之該第一部分發送至該計算設備。回應於該智慧卡讀取器已經由一使用者介面而接收到該查問，其將該回應之至少該第二部分經由該使用者介面而呈現至一使用者。

## 六、英文發明摘要：

In an authentication server, information representing a first part of a response to a challenge is received during the authentication preparation phase. The challenge and the first part of the response are stored for further use. The challenge is resent and information representing a second part of the response to the challenge is received during a modified authentication phase. The first and second parts of the response are checked against the challenge for authenticating the user. In a smartcard reader, the response received from the smartcard is sent to a computing device, when the smartcard reader received the challenge via an interface to the computing device during normal authentication. In response to the smartcard reader having received the challenge via the interface to the computing device during an authentication preparation phase, the smartcard reader sends the first part of the response to the computing device. In response to the smartcard reader having received the challenge via a user interface, it presents at least the second part of the response to a user via the user interface.

## 七、指定代表圖：

(一)本案指定代表圖為：第（ 3 ）圖。

(二)本代表圖之元件符號簡單說明：

| | |
|---|---|
| 300 | 第一計算設備 |
| 310 | 第一使用者介面 |
| 320 | 第一處理器 |
| 330 | 第一網路介面 |
| 340 | USB埠 |
| 400 | 第二計算設備 |
| 410 | 第二使用者介面 |
| 420 | 第二處理器 |
| 430 | 第二網路介面 |
| 500 | 伺服器 |
| 550 | 鑑認伺服器 |
| 600 | 網路 |
| 700 | 行動讀卡器 |
| 710 | 接針墊 |
| 720 | 顯示器 |
| 800 | 智慧卡 |
| 850 | 微處理器 |
| 900 | 使用者 |

## 八、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

（無）

## 九、發明說明：

【發明所屬之技術領域】

本發明係關於一種用於處理鑑認資訊之智慧卡讀取器及鑑認伺服器，以及係關於用於處理鑑認資訊之相應方法及電腦程式產品。

【先前技術】

對電腦網路中之安全使用者鑑認(較佳地對網際網路服務)的需求非常高。當必須保護個人資料、銀行帳戶或健康資料時，密碼並非很安全且可能不會實現所需安全標準。如(例如)電子符記之其他解決方案為高度專屬的。

為了克服安全性及互用性中之問題，已開發智慧卡技術，其組合標準順應性與極安全演算法。

智慧卡對於使用者鑑認之使用被視為強鑑認形式且組合使用者所具有之某物(亦即，智慧卡)與使用者所知曉之某物(例如，PIN)之使用，以提供被稱為兩因素鑑認之鑑認。智慧卡基本上為小塑膠卡、約為普通信用卡之尺寸，且通常含有小嵌入式電腦晶片(亦即，微晶片)而非傳統信用卡中所提供之磁條。智慧卡為簽名卡。智慧卡上所給出之一些認證用於簽名且一些認證則用於鑑認。

已知的是提供互動式智慧卡登入以及遠端智慧卡鑑認。使用者具有經由其智慧卡而存取遠端機器且互動式地輸入PIN以登入之能力，正如其實體地走向遠端機器之控制台一般。遠端智慧卡鑑認及互動式登入不需要任何類型之智慧卡中間軟體，且甚至不需要附接至遠端機器之智慧卡讀

取器。

由於以上所提及之原因，智慧卡正變得愈來愈風行。若干國家之官員正考慮向其公民發行身份或鑑認智慧卡。此外，銀行正發行支援數位簽名之增加數目之卡。智慧卡可用於網際網路服務中之鑑認，例如，以智慧卡之原始發行者留意鑑認且接著向服務提供者通知鑑認之結果的方式。

然而，在將智慧卡鑑認用於網際網路中之服務時存在一些問題。一原因在於：大多數人將一個以上電腦用於其在網際網路上之敏感交易。因此，必須針對所使用電腦中之每一者而安裝智慧卡讀取器。但，即使當將智慧卡讀取器及適當軟體安裝於每一電腦處時，使用者亦不知曉電腦是否可被信任或智慧卡上之敏感資料是否將被不希望地存取。商業認證智慧卡讀取器僅針對被使用者信任且控制之環境而經認證。

本發明之一目標為尤其針對網際網路服務之需求而在電腦網路內提供安全使用者鑑認。本發明之另一目標為尤其在電腦網路之非被信任電腦上執行時在電腦網路內提供安全使用者鑑認。

【發明內容】

本發明提供一種用於在智慧卡讀取器中處理鑑認資訊之方法，方法包含以下步驟：

在智慧卡讀取器中接收查問且將查問發送至智慧卡，

自智慧卡接收對查問之回應，該回應具有至少第一部分及第二部分，

回應於已在正常鑑認期間經由至計算設備之介面而在智慧卡讀取器中接收到查問，將該回應發送至該計算設備，

回應於已在鑑認準備階段期間經由至計算設備之介面而在智慧卡讀取器中接收到查問，將回應之第一部分發送至計算設備，及

回應於已經由智慧卡讀取器之使用者介面而在智慧卡讀取器中接收到查問，將回應之至少第二部分經由使用者介面而呈現至使用者。

當接收到查問時，智慧卡讀取器將回應發送至計算設備或將回應之第一部分發送至計算設備或將顯示回應之第二部分。發送對查問之回應為如已經藉由根據目前技術狀態之方法而實踐的普通狀況。發送回應之第一部分與計算設備經由介面而能夠存取智慧卡讀取器一起發生且為藉由根據本發明之方法而提供的選項。發送回應之第二部分與智慧卡讀取器經由使用者所起始之輸入過程而接收查問一起發生。

本發明進一步提供一種用於在鑑認伺服器中處理鑑認資訊之方法，方法包含以下步驟：

在鑑認準備階段期間發送查問以用於鑑認使用者，

回應於在鑑認準備階段期間發送查問，接收表示對查問之回應之第一部分的資訊，

在鑑認準備階段期間儲存查問及回應之第一部分以用於在經修改鑑認期間之進一步使用，

在經修改鑑認期間重新發送查問以用於鑑認使用者，

回應於重新發送查問，接收表示對查問之回應之第二部分的資訊，及

對照查問來檢查回應之第一部分及第二部分且在回應證明為有效時在經修改鑑認期間成功地鑑認使用者。

鑑認伺服器將在鑑認準備階段期間發送查問或將在經修改鑑認期間重新發送查問以用於鑑認使用者。提供一種用於觸發預期鑑認步驟之預定義準則，其為在鑑認準備階段中準備鑑認或在經修改鑑認期間完成鑑認。

準則可能由觸發鑑認伺服器重新發送用於經修改鑑認之查問或阻止鑑認伺服器發送用於鑑認準備階段之新查問的模組提供。

如用於本發明之術語"計算設備"包含個人電腦、票券(ticket)、自動售貨及提款機、行動電話及其類似物且被儘可能廣泛地解譯。

根據本發明之方法的優點在於：智慧卡與非被信任計算設備之使用不會將對敏感資訊之存取提供於非被信任電腦處，因為在未將智慧卡連接至非被信任電腦的情況下使用智慧卡。

使用者可(例如)具備用於戶外使用之包含小鍵盤及表示構件(較佳地為顯示器)的行動智慧卡讀取器，其較佳地具有可再充電電池以用於網際網路咖啡館。在電腦螢幕上向使用者顯示查問且使用者借助於小鍵盤而將查問輸入於智慧卡讀取器中。智慧卡加密查問且回應之第二部分顯示於智慧卡讀取器顯示器上。使用者在電腦之使用者介面處輸

入回應之第二部分。當使用者已執行亦被稱為鑑認準備階段之"本籍鑑認"(亦即，以待信任之計算設備之鑑認)時，回應之第一部分已經儲存於鑑認伺服器中。

如用於本發明之術語"顯示器"應在其最廣泛意義上被理解且包含對使用者之感官知覺(例如，他的視覺、聽覺及/或觸覺)可存取之各種各類的表示構件。因此，例如，"顯示查問或回應"亦包含經由耳機之音訊顯示。

當使用者正使用智慧卡及非被信任電腦時，再次使用如同被信任電腦之情況的相同查問。使用者將較佳地具有合理長度之查問輸入至智慧卡，其再次計算回應。使用者經有利地展示回應之第二部分，其尚未在鑑認準備階段中以待信任之計算設備進行傳輸。使用者接著輸入傳輸至鑑認伺服器的回應之第二部分。鑑認伺服器組合回應之第一部分與第二部分且檢查經組合回應是否有效。

在對查問之回應為數位序列的狀況下，回應之第一部分及第二部分各自為可相互補充之此等數位的選擇。"組合"回應之第一部分與第二部分則意謂獲得完整回應。

使用者可在鑑認準備階段中預定義遮罩，其判定進行選擇之方式。舉例而言，使回應為40個數位之序列且遮罩實施以下類型之交替型樣：回應之第一部分包含第一、第三、第五等等數位，且回應之第二部分包含第二、第四等等數位。遮罩亦可實施另一型樣：回應之第一部分包含第一至第三十數位，且回應之第二部分包含第三十一至最後數位。實際上，存在許多替代選項。若第二回應包含不多

於十個數位，則戶外鑑認在僅少許數位必須在小鍵盤中被輸入的意義上為使用者親和的。

根據本發明之結構的安全性依靠兩個鑑認因素：智慧卡及私用鑑認密鑰連同儲存於智慧卡上之認證。因此，不使用專屬認證，且鑑認伺服器可使用任何給定基礎結構(如(例如)目錄及撤回服務)以檢查智慧卡及私用鑑認密鑰連同認證之有效性。

此結構之安全性質為極佳的。在對鑑認伺服器之未經授權存取的狀況下，侵入者將發現經儲存查問及回應之第一部分，其不會向他提供用於鑑認之完整資訊。若計算設備在資料傳輸期間受到攻擊，則侵入者將僅發現對他無用的回應之第一部分或第二部分。無相關資料儲存於智慧卡讀取器本身上。若某人在計算設備處監視使用者，則只要每一查問僅被使用一次，所獲得資訊就無用。

因此，儘管原則上有可能將一查問使用若干次，但儲存於鑑認伺服器中之每一查問僅被使用一次。

在方法之一較佳實施例中，在經由待信任之計算設備而請求對電腦網路之存取的步驟之後，至少一查問經產生且儲存於鑑認伺服器中。

術語"至少一查問"包含產生若干查問以便維持查問之一定供應的狀況。此在使用者暫時不能夠存取待信任之計算設備但必須將非被信任之計算設備使用若干次的狀況下為有利的。通常，8位數足以建置查問。每當使用者自戶外(亦即，自非被信任計算設備)請求鑑認時，鑑認伺服器發

送8位數中之一者。

在方法之另一較佳實施例中，在自鑑認伺服器接收查問之後，查問在智慧卡上經加密。

查問有利地在智慧卡讀取器之小鍵盤中輸入PIN之後在智慧卡上以私用鑑認密鑰進行加密。

檢查回應是否有效之步驟有利地包含解密經加密回應之第一部分及第二部分且對照查問來檢查經加密回應之第一部分及第二部分的步驟。

經加密回應之第一部分及第二部分較佳地以使用者之公用密鑰進行解密，亦即，應用不對稱密鑰設計。

在方法之非常實用的實施例中，回應之第二部分包含選自完整回應之有限數目的數位，較佳地在6個數位與12個數位之間。在此狀況下，尤其較佳的是自完整回應選擇最後6至12個數位。此有限數目的數位允許由使用者所進行之方便的輸入。又，查問可包含有限數目的數位，例如，在6個數位與12個數位之間。數位之數目為安全性需求對比實用性及舒適性需求之間的折衷。

根據本發明之方法非常適合於在對照查問來檢查回應之第一部分及第二部分且回應證明為有效時鑑認任何使用者。

本發明亦提供一種含有用於在智慧卡讀取器中處理鑑認資訊之電腦可執行指令的電腦程式產品及一種含有用於在鑑認伺服器中處理鑑認資訊之電腦可執行指令的電腦程式產品，電腦程式產品中之每一者對應於如上文所描述之方

法中之一者。

本發明進一步提供一種用於處理鑑認資訊之智慧卡讀取器，智慧卡讀取器包含

使用者介面組件，其用於將資訊呈現至使用者且自使用者接收輸入資訊；

第一組件，其用於將介面提供至計算設備以用於至少自計算設備接收查問；

第二組件，其用於將介面提供至智慧卡以用於至少將查問發送至智慧卡且自智慧卡接收對查問之回應，該回應具有至少第一部分及第二部分；及

處理組件，其用於控制智慧卡讀取器之操作，處理組件使：

第一組件回應於智慧卡讀取器已在正常鑑認期間經由至計算設備之介面而接收到各別查問而將自智慧卡所接收之回應發送至該計算設備；

第一組件回應於智慧卡讀取器已在鑑認準備階段期間經由至計算設備之介面而接收到各別查問而將自智慧卡所接收之回應之第一部分發送至計算設備；且

使用者介面組件回應於智慧卡讀取器已經由使用者介面組件而接收到各別查問而經由使用者介面組件來呈現自智慧卡所接收之回應之至少第二部分。

本發明另外提供一種用於處理鑑認資訊之計算系統(例如，鑑認伺服器)，計算系統包含

用於在鑑認準備階段期間發送查問以用於鑑認使用者

的構件，

用於回應於在鑑認準備階段期間發送查問而接收表示對查問之回應之第一部分的資訊的構件，

用於在鑑認準備階段期間儲存查問及回應之第一部分以用於在經修改鑑認期間之進一步使用的構件，

用於在經修改鑑認期間重新發送查問以用於鑑認使用者的構件，

用於回應於重新發送查問而接收表示對查問之回應之第二部分的資訊的構件，及

用於對照查問來檢查回應之第一部分及第二部分且在回應證明為有效時在經修改鑑認期間成功地鑑認使用者的構件。

智慧卡讀取器經調適以在第一步驟中發送對自鑑認伺服器所傳輸之查問之回應之第一部分且在第二步驟中顯示對由使用者所輸入之查問之回應之第二部分。

在一較佳實施例中，智慧卡讀取器及鑑認伺服器各自經調適以用於執行如上文所描述之方法中之一者。

智慧卡之實例為來自Telesec、Signtrust、TC Trustcenter及D-Trust之簽名卡。許多卡提供用於鑑認之密鑰及用於簽名文件之密鑰。兩種密鑰皆可在演算法態樣下被使用且應根據智慧卡之密鑰使用策略加以選擇。

當結合以下描述及隨附圖式來考慮時，可更好地瞭解且理解本發明之此等及其他態樣及目標。然而，應理解，雖然以下描述指示本發明之較佳實施例及其許多特定細節，

但其係經由說明而非限制之方式被給出。可在不偏離本發明之精神的情況下在本發明之範疇內進行許多改變及修改，且本發明包括所有此等修改。

本發明可採用完全硬體實施例、完全軟體實施例或含有硬體與軟體元件兩者之實施例的形式。在一較佳實施例中，本發明以軟體加以實施，軟體包括(但不限於)韌體、常駐軟體、微碼，等等。

此外，本發明可採用自電腦可用媒體或電腦可讀媒體可存取之電腦程式產品的形式，電腦可用媒體或電腦可讀媒體提供由電腦或任何指令執行系統使用或結合電腦或任何指令執行系統而使用之程式碼。為了此描述之目的，電腦可用或電腦可讀媒體可為可含有、儲存、傳達、傳播或輸送由指令執行系統、裝置或設備使用或結合指令執行系統、裝置或設備而使用之程式的任何裝置。

媒體可為電子、磁性、光學、電磁、紅外或半導體系統(或裝置或設備)或傳播媒體。電腦可讀媒體之實例包括半導體或固態記憶體、磁帶、可移除式電腦碟片、隨機存取記憶體(RAM)、唯讀記憶體(ROM)、硬質磁碟及光碟。光碟之當前實例包括唯讀光碟(CD-ROM)、可重複錄寫光碟(CD-R/W)及數位多功能光碟(DVD)。

適合於儲存及/或執行程式碼之資料處理系統將包括至少一處理器，其直接耦接至記憶體元件或經由系統匯流排而間接耦接至記憶體元件。記憶體元件可包括在程式碼之實際執行期間所使用之區域記憶體、大容量儲存器及快取

記憶體，快取記憶體提供至少某一程式碼之臨時儲存，以便減少在執行期間必須自大容量儲存器擷取碼之次數。

輸入/輸出或I/O設備(包括(但不限於)鍵盤、顯示器、指向設備，等等)可直接耦接至系統或經由介入之I/O控制器而耦接至系統。

網路配接器亦可耦接至系統以使資料處理系統能夠經由介入之私用或公用網路而變得耦接至其他資料處理系統或遠端印表機或儲存設備。數據機、電纜數據機及乙太網路卡僅為當前可用類型之網路配接器中的少數幾種。

【實施方式】

將參看圖式而自以下詳細描述更好地理解本發明。

圖1為說明藉由借助於行動智慧卡讀取器而將智慧卡連接至第一計算設備而經由第一計算設備來請求對電腦網路之存取及自鑑認伺服器接收查問且將回應之第一部分傳輸至鑑認伺服器之步驟的圖表。

設定為由垂直虛線所指示之用戶端/伺服器介面。用戶端在圖1中未圖示之第一計算設備上執行。用戶端側包含使用者、智慧卡、瀏覽器/應用程式及讀卡器，讀卡器可經由用於資料交換且最終用於裝載讀卡器之電池的USB(通用串列匯流排)埠而連接至第一計算設備，且伺服器側包含鑑認伺服器。

在第一步驟中，如由箭頭1所指示建立瀏覽器/應用程式與鑑認伺服器之間的SSL(安全通訊端層)連接。例如，藉由SSL連接，可避免"中間人攻擊"(man-in-the-middle-

attacks)。

在下一步驟中，使用者請求新查問之產生。將請求如由箭頭2所指示定址至瀏覽器/應用程式且如由箭頭3所指示傳送至鑑認伺服器。應用程式伺服器因此產生且儲存一或多個查問4。

在另一步驟中，將查問4如由箭頭5及6所指示經由瀏覽器/應用程式而發送至讀卡器。將查問4如由箭頭7所展示自讀卡器傳送至智慧卡。

使用者根據箭頭8而在讀卡器之接針墊中輸入PIN。將PIN發送至智慧卡，見箭頭9。以使用者之私用鑑認密鑰來加密查問4。在智慧卡上產生被稱為回應之經加密查問10。

智慧卡根據箭頭11而將回應發送至讀卡器，且將回應之第一部分自讀卡器經由瀏覽器/應用程式而發送至鑑認伺服器，見箭頭12及13。在鑑認伺服器中儲存回應之第一部分14。

圖1所說明之過程可根據箭頭15而被重複n次(n為整數)，以便儲存對於n個查問4之回應之第一部分14。

如圖1所描述之過程可被視為如圖2所描述之過程的準備過程。

準備過程可由使用者起始或自動地起始，例如，當經儲存未用查問之供應降至低於特定極限時。亦可提供用以(例如)藉由發送電子郵件訊息來提醒使用者起始準備過程之自動常式。

其在智慧卡允許在使用者已輸入他的PIN之後鑑認多次時使準備過程簡易。

在已成功地執行以被信任計算設備之準備過程之後，可將所連接智慧卡讀取器切換至"戶外鑑認"，以便在作為預設狀況的以非被信任計算設備之鑑認過程內起作用。

圖2為說明經由第二計算設備而請求對電腦網路之存取及將智慧卡連接至行動智慧卡讀取器且自鑑認伺服器接收查問及傳送回應之第二部分(因此，鑑認伺服器組合回應之第一部分與第二部分且檢查回應是否有效)之步驟的圖表。

圖2中之設定為如在圖1中由垂直虛線所指示之用戶端/伺服器介面。在圖2中未圖示之第二計算設備上執行用戶端。用戶端側包含使用者、智慧卡、瀏覽器及未連接至第二計算設備之讀卡器，且伺服器側包含鑑認伺服器。

在第一步驟中，使用者希望鑑認，見箭頭21，且因此，如由箭頭22所指示建立瀏覽器與鑑認伺服器之間的SSL(安全通訊端層)連接。

在下一步驟中，鑑認伺服器如由箭頭23所說明將經假定等同於圖1中之查問4的經儲存查問40發送至瀏覽器，且瀏覽器向使用者顯示經儲存查問40，見箭頭24。

在另一步驟中，使用者如由箭頭25所指示在讀卡器中輸入查問40，且接著，使用者如由箭頭26所指示在讀卡器中輸入PIN。

讀卡器如由箭頭27所指示將查問40發送至智慧卡。以私

用鑑認密鑰來加密查問40，且將經假定等同於圖1中之經加密查問10的經加密查問20(兩者皆被稱為回應)儲存於智慧卡上。

智慧卡根據箭頭28而將回應發送至讀卡器，且將回應之第二部分根據箭頭29而自讀卡器向使用者顯示。

接著，使用者輸入經由瀏覽器而發送至鑑認伺服器的回應之第二部分，見箭頭30及31。

鑑認伺服器根據1.)而組合回應之第一部分與第二部分，接著根據2.)而以使用者之公用密鑰來解密回應，接著根據3.)而比較經解密回應與查問。若經解密回應等同於查問，則根據4.)而鑑認使用者。

如圖2所描述之過程應被視為戶外鑑認，其係基於如圖1所描述之準備過程。

圖3為用於本發明之使用之例示性環境的示意性說明。

第一計算設備300及第二計算設備400經由網路600而連接至伺服器500。第一計算設備300包含第一使用者介面310、第一處理器320及第一網路介面330。第二計算設備400包含第二使用者介面410、第二處理器420及第二網路介面430。伺服器500包含鑑認伺服器550。行動讀卡器700包含接針墊710及顯示器720且經調適以收納包含微處理器850之智慧卡800。微處理器850經調適以加密及解密查問。行動讀卡器700可如由虛線所指示經由USB埠340而連接至第一計算設備300。若第一計算設備300為待由使用者900信任之計算設備，則執行如圖1所描述之過程。當在第

二計算設備400處工作但未連接至第二計算設備400時，可使用行動讀卡器700。若第二計算設備400為將未由使用者900信任之計算設備，則執行如圖2所描述之過程。

應注意，本文中所描述之態樣及實施例可使用根據本說明書之教示而程式化的機器(例如，通用計算設備)加以方便地實施，此將為熟習電腦技術者所明白。適當軟體編碼可由熟練程式設計員基於本揭示案之教示容易地準備，此將為熟習軟體技術者所明白。

此軟體可為使用機器可讀媒體之電腦程式產品。機器可讀媒體可為能夠儲存及/或編碼由機器(例如，通用計算設備)執行之指令序列且使機器執行本文中所描述之方法及/或實施例中之任一者的任何媒體。機器可讀媒體之實例包括(但不限於)：磁碟，例如，習知軟碟、硬驅動碟；光碟，例如，"CD"，諸如，可讀、可寫及/或可重複錄寫CD；"DVD"，諸如，可讀、可寫及/或可重複錄寫DVD；磁光碟；唯讀記憶體"ROM"設備；隨機存取記憶體"RAM"設備；磁卡；光卡；固態記憶體設備，例如，快閃記憶體、EPROM、EEPROM；及其任何組合。如本文中所使用之機器可讀媒體預期包括單一媒體以及實體獨立媒體之集合，諸如，緊密光碟或一或多個硬碟機結合電腦記憶體之集合。

通用計算設備之實例包括(但不限於)電腦工作站、終端電腦、伺服器電腦、掌上型設備(例如，平板電腦、個人數位助理"PDA"、行動電話，等等)、網路電氣設備、網路

路由器、網路交換器、網路橋接器、能夠執行規定待由彼機器採取之行動之指令序列的任何機器，及其任何組合。在一實例中，通用計算設備可包括公共資訊查詢站(kiosk)及/或包括於公共資訊查詢站中。

雖然前文已參考本發明之特定實施例，但熟習此項技術者應瞭解，可在不偏離本發明之原理及精神的情況下進行此等實施例之改變，本發明之範疇係由隨附申請專利範圍定義。

【圖式簡單說明】

圖1為說明藉由借助於行動智慧卡讀取器而將智慧卡連接至第一計算設備而經由第一計算設備來請求對電腦網路之存取及自鑑認伺服器接收查問且將回應之第一部分傳輸至鑑認伺服器之步驟的圖表；

圖2為說明經由第二計算設備而請求對電腦網路之存取及將智慧卡連接至行動智慧卡讀取器且自鑑認伺服器接收查問及傳送回應之第二部分(因此，鑑認伺服器組合回應之第一部分與第二部分且檢查回應是否有效)之步驟的圖表；

圖3為用於本發明之使用之例示性環境的示意性說明。

【主要元件符號說明】

| | |
|---|---|
| 300 | 第一計算設備 |
| 310 | 第一使用者介面 |
| 320 | 第一處理器 |
| 330 | 第一網路介面 |

| | |
|---|---|
| 340 | USB埠 |
| 400 | 第二計算設備 |
| 410 | 第二使用者介面 |
| 420 | 第二處理器 |
| 430 | 第二網路介面 |
| 500 | 伺服器 |
| 550 | 鑑認伺服器 |
| 600 | 網路 |
| 700 | 行動讀卡器 |
| 710 | 接針墊 |
| 720 | 顯示器 |
| 800 | 智慧卡 |
| 850 | 微處理器 |
| 900 | 使用者 |

# 十、申請專利範圍：

1. 一種用於在一智慧卡讀取器中處理鑑認資訊之方法，該方法包含：

經由一第一計算設備由一智慧卡讀取器接收一來自一鑑認伺服器之查問，該第一計算設備經由一網路連接至該鑑認伺服器；

在該接收該查問之後，該智慧卡讀取器將該查問傳送至一智慧卡；

在該傳送該查問至該智慧卡之後，該智慧卡讀取器從該智慧卡接收對該查問之一回應，該回應包含該查問之一加密，該回應包含一第一部份及一第二部份，該查問之該加密係經由使用一使用者之一私用鑑認密鑰而產生；

回應於該智慧卡讀取器已經從該智慧卡接收到該回應，該智慧卡讀取器經由該第一計算設備將該回應之該第一部份發送至該鑑認伺服器；

在該將該回應之該第一部份發送至該鑑認伺服器之後，該智慧卡讀取器經由一第二計算設備從該鑑認伺服器獲得該查問，該第二計算設備經由該網路連接至該鑑認伺服器，該第二計算設備及該第一計算設備為不同的計算設備；

在該獲得該查問之後，該智慧卡讀取器將該查問提供給該智慧卡；

在該將該查問提供給該智慧卡之後，該智慧卡讀取器

從該智慧卡獲得該回應；

回應於該智慧卡讀取器已經從該智慧卡獲得該回應，經由該智慧卡讀取器上之一使用者介面將該回應之該第二部分顯示給該使用者。

2. 如請求項1之方法，該方法進一步包含：

在該將該查問傳送至該智慧卡之後，該智慧卡讀取器在該智慧卡讀取器上經由該使用者接收該使用者之一個人識別號（PIN）之一第一條目；及

回應於該接收該PIN之該第一條目，該智慧卡讀取器將該PIN之該第一條目發送至該智慧卡，

其中該從該智慧卡接收該回應係在該回應已經由該智慧卡回應於該智慧卡已經從該智慧卡讀取器接收到該PIN之該第一條目而產生之後執行。

3. 如請求項2之方法，該方法進一步包含：

在該將該查問提供給該智慧卡之後，該智慧卡讀取器在該該智慧卡讀取器上經由該使用者接收該PIN之一第二條目；且

回應於該接收該PIN之該第二條目，該智慧卡讀取器將該PIN之該第二條目發送至該智慧卡，

其中該從該智慧卡獲得該回應係在該回應已經由該智慧卡回應於該智慧卡已經從該智慧卡讀取器接收到該PIN之該第二條目而產生之後執行。

4. 如請求項1之方法，該方法進一步包含：

回應於將該回應之該第二部分顯示給該使用者，經由

該使用者接收該回應之該第二部分之一條目；

回應於該接收該回應之該第二部分，經由該第二計算設備將該回應之該第二部分發送至該鑑認伺服器。

5. 如請求項4之方法，該回應由該第一部份及該第二部份組成，該方法進一步包含：

在該鑑認伺服器已經接收經由該第二計算設備發送之該回應之該第二部分之後，該鑑認伺服器經由將回應之該第一及第二部分組合而產生一組合回應；

在該產生該組合回應之後，該鑑認伺服器解密該組合回應；且

該鑑認伺服器判定經解密之組合回應等於該查問。

6. 如請求項1之方法，其中該第一計算設備係一被該使用者信任之被信任計算設備，且其中該第二計算裝置係一不被該使用者信任之非被信任計算設備。

7. 一種電腦程式產品，其包含一電腦可讀取之具有儲存於其中之電腦可讀取程式碼之有形的物理儲存設備，該程式碼經組態以經由一資料處理系統之至少一處理器執行，以實施一種用於處理該資料處理系統包含之一智慧卡讀取器中之鑑認資訊之方法，該方法包含：

經由一第一計算設備由一智慧卡讀取器接收一來自一鑑認伺服器之查問，該第一計算設備經由一網路連接至該鑑認伺服器；

在該接收該查問之後，該智慧卡讀取器將該查問傳送至一智慧卡；

在該傳送該查問至該智慧卡之後，該智慧卡讀取器從該智慧卡接收對該查問之一回應，該回應包含該查問之一加密，該回應包含一第一部份及一第二部份，該查問之該加密係經由使用一使用者之一私用鑑認密鑰而產生；

回應於該智慧卡讀取器已經從該智慧卡接收到該回應，該智慧卡讀取器經由該第一計算設備將該回應之該第一部份發送至該鑑認伺服器；

在該將該回應之該第一部份發送至該鑑認伺服器之後，該智慧卡讀取器經由一第二計算設備從該鑑認伺服器獲得該查問，該第二計算設備經由該網路連接至該鑑認伺服器，該第二計算設備及該第一計算設備為不同的計算設備；

在該獲得該查問之後，該智慧卡讀取器將該查問提供給該智慧卡；

在該將該查問提供給該智慧卡之後，該智慧卡讀取器從該智慧卡獲得該回應；

回應於該智慧卡讀取器已經從該智慧卡獲得該回應，經由該智慧卡讀取器上之一使用者介面將該回應之該第二部分顯示給該使用者。

8. 如請求項7之電腦程式產品，其中該方法進一步包含：

在該將該查問傳送至該智慧卡之後，該智慧卡讀取器在該智慧卡讀取器上經由該使用者接收該使用者之一個人識別號（PIN）之一第一條目；及

回應於該接收該PIN之該第一條目，該智慧卡讀取器將該PIN之該第一條目發送至該智慧卡，

其中該從該智慧卡接收該回應係在該回應已經由該智慧卡回應於該智慧卡已經從該智慧卡讀取器接收到該PIN之該第一條目而產生之後執行。

9. 如請求項8之電腦程式產品，其中該方法進一步包含：

在該將該查問提供給該智慧卡之後，該智慧卡讀取器在該該智慧卡讀取器上經由該使用者接收該PIN之一第二條目；且

回應於該接收該PIN之該第二條目，該智慧卡讀取器將該PIN之該第二條目發送至該智慧卡，

其中該從該智慧卡獲得該回應係在該回應已經由該智慧卡回應於該智慧卡已經從該智慧卡讀取器接收到該PIN之該第二條目而產生之後執行。

10. 如請求項7之電腦程式產品，其中該方法進一步包含：

回應於將該回應之該第二部分顯示給該使用者，經由該使用者接收該回應之該第二部分之一條目；

回應於該接收該回應之該第二部分，經由該第二計算設備將該回應之該第二部分發送至該鑑認伺服器。

11. 如請求項10之電腦程式產品，該回應由該第一部份及該第二部份組成，該方法進一步包含：

在該鑑認伺服器已經接收經由該第二計算設備發送之該回應之該第二部分之後，該鑑認伺服器經由將回應之該第一及第二部分組合而產生一組合回應；

在該產生該組合回應之後，該鑑認伺服器解密該組合回應；且

該鑑認伺服器判定經解密之組合回應等於該查問。

12. 如請求項7之電腦程式產品，其中該第一計算設備係一被該使用者信任之被信任計算設備，且其中該第二計算裝置係一不被該使用者信任之非被信任計算設備。

13. 一資料處理系統，其包含至少一處理器、一耦接至該處理器之電腦可讀取記憶體單元、及耦接至該處理器之一有形的物理儲存設備，該儲存設備儲存經組態以由該至少一處理器經由該記憶體單元執行之程式碼，以實施一種用於處理該資料處理系統包含之一智慧卡讀取器中之鑑認資訊之方法，該方法包含：

經由一第一計算設備由一智慧卡讀取器接收一來自一鑑認伺服器之查問，該第一計算設備經由一網路連接至該鑑認伺服器；

在該接收該查問之後，該智慧卡讀取器將該查問傳送至一智慧卡；

在該傳送該查問至該智慧卡之後，該智慧卡讀取器從該智慧卡接收對該查問之一回應，該回應包含該查問之一加密，該回應包含一第一部份及一第二部份，該查問之該加密係經由使用一使用者之一私用鑑認密鑰而產生；

回應於該智慧卡讀取器已經從該智慧卡接收到該回應，該智慧卡讀取器經由該第一計算設備將該回應之該

第一部份發送至該鑑認伺服器；

在該將該回應之該第一部份發送至該鑑認伺服器之後，該智慧卡讀取器經由一第二計算設備從該鑑認伺服器獲得該查問，該第二計算設備經由該網路連接至該鑑認伺服器，該第二計算設備及該第一計算設備為不同的計算設備；

在該獲得該查問之後，該智慧卡讀取器將該查問提供給該智慧卡；

在該將該查問提供給該智慧卡之後，該智慧卡讀取器從該智慧卡獲得該回應；

回應於該智慧卡讀取器已經從該智慧卡獲得該回應，經由該智慧卡讀取器上之一使用者介面將該回應之該第二部分顯示給該使用者。

14.如請求項13之資料處理系統，其中該方法進一步包含：

在該將該查問傳送至該智慧卡之後，該智慧卡讀取器在該智慧卡讀取器上經由該使用者接收該使用者之一個人識別號（PIN）之一第一條目；及

回應於該接收該PIN之該第一條目，該智慧卡讀取器將該PIN之該第一條目發送至該智慧卡，

其中該從該智慧卡接收該回應係在該回應已經由該智慧卡回應於該智慧卡已經從該智慧卡讀取器接收到該PIN之該第一條目而產生之後執行。

15.如請求項14之資料處理系統，其中該方法進一步包含：

在該將該查問提供給該智慧卡之後，該智慧卡讀取器

在該該智慧卡讀取器上經由該使用者接收該PIN之一第二條目；且

回應於該接收該PIN之該第二條目，該智慧卡讀取器將該PIN之該第二條目發送至該智慧卡，

其中該從該智慧卡獲得該回應係在該回應已經由該智慧卡回應於該智慧卡已經從該智慧卡讀取器接收到該PIN之該第二條目而產生之後執行。

16.如請求項13之資料處理系統，其中該方法進一步包含：

回應於將該回應之該第二部分顯示給該使用者，經由該使用者接收該回應之該第二部分之一條目；

回應於該接收該回應之該第二部分，經由該第二計算設備將該回應之該第二部分發送至該鑑認伺服器。

17.如請求項16之資料處理系統，該回應由該第一部份及該第二部份組成，該方法進一步包含：

在該鑑認伺服器已經接收經由該第二計算設備發送之該回應之該第二部分之後，該鑑認伺服器經由將回應之該第一及第二部分組合而產生一組合回應；

在該產生該組合回應之後，該鑑認伺服器解密該組合回應；且

該鑑認伺服器判定經解密之組合回應等於該查問。

18.如請求項13之資料處理系統，其中該第一計算設備係一被該使用者信任之被信任計算設備，且其中該第二計算裝置係一不被該使用者信任之非被信任計算設備。

# 十一、圖式：

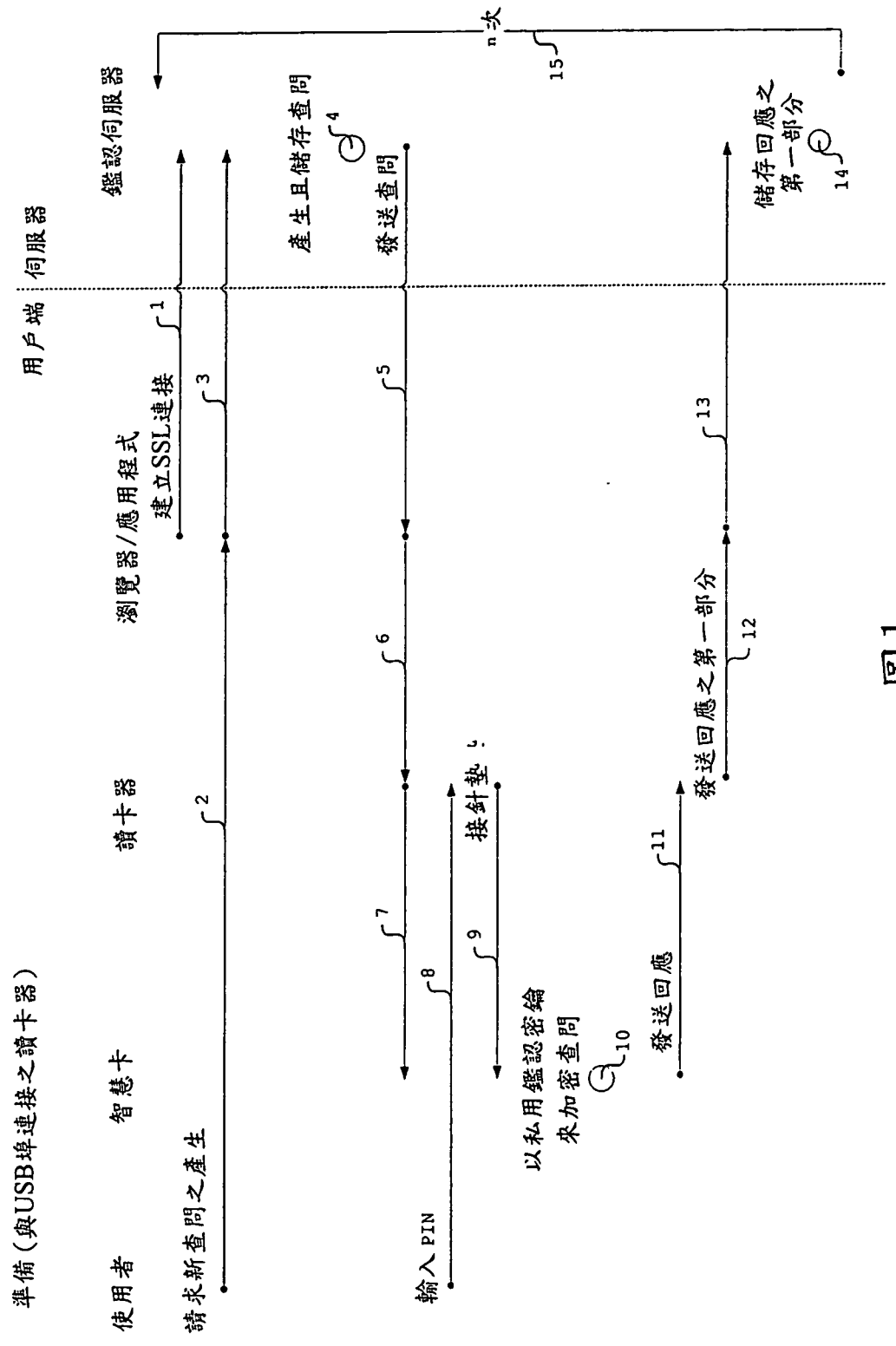
準備（與USB埠連接之讀卡器）
用戶端
伺服器
使用者
智慧卡
讀卡器
瀏覽器/應用程式
鑑認伺服器
建立SSL連接
請求新查問之產生
產生且儲存查問
發送查問
輸入PIN
接針墊
以私用鑑認密鑰
來加密查問
發送回應
發送回應之第一部分
儲存回應之第一部分
n次
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15

圖1

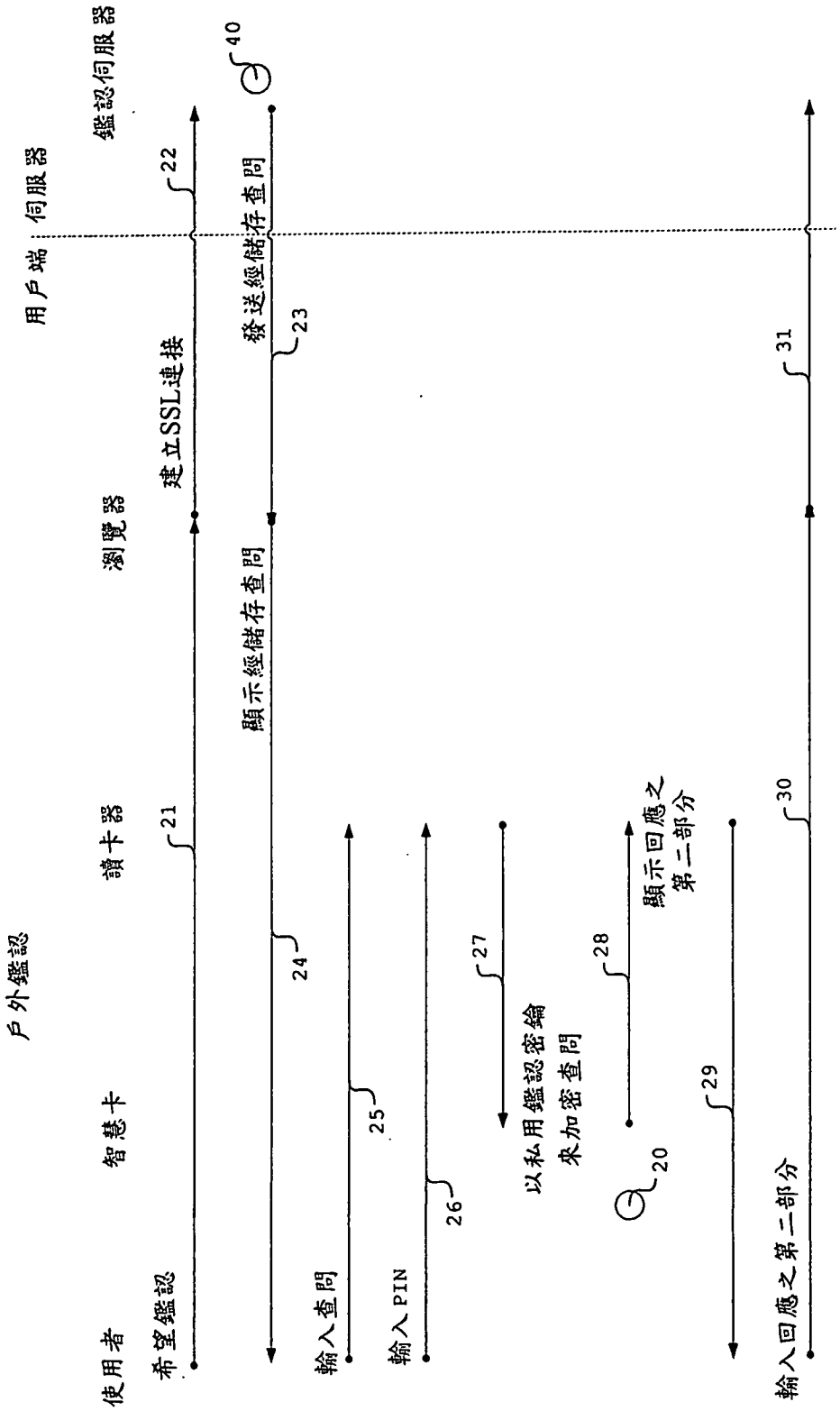
戶外鑑認
使用者
智慧卡
讀卡器
瀏覽器
用戶端
伺服器
鑑認伺服器
布望鑑認
21
建立SSL連接
22
顯示經儲存查問
40
發送經儲存查問
23
24
輸入查問
25
輸入PIN
26
以私用鑑認密鑰
來加密查問
27
20
28
顯示回應之
第二部分
29
輸入回應之第二部分
30
31
1.)組合回應之第一部分與第二部分
2.)以使用者之公用密鑰來解密回應
3.)比較經解密回應與查問
4.)若等同，則鑑認使用者

圖2

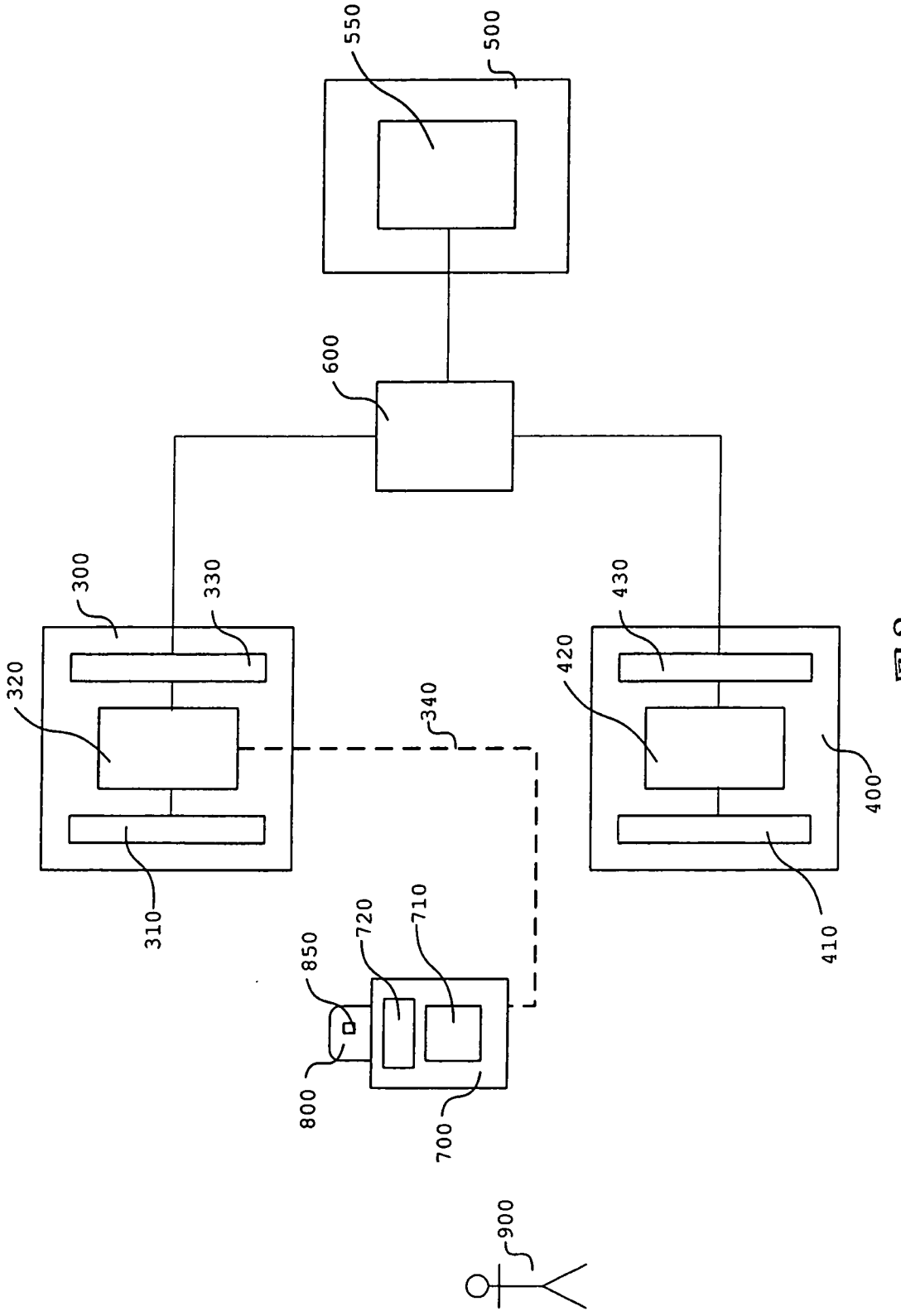
550
500
600
300
330
320
340
430
420
400
310
410
850
720
710
800
700
900

圖3