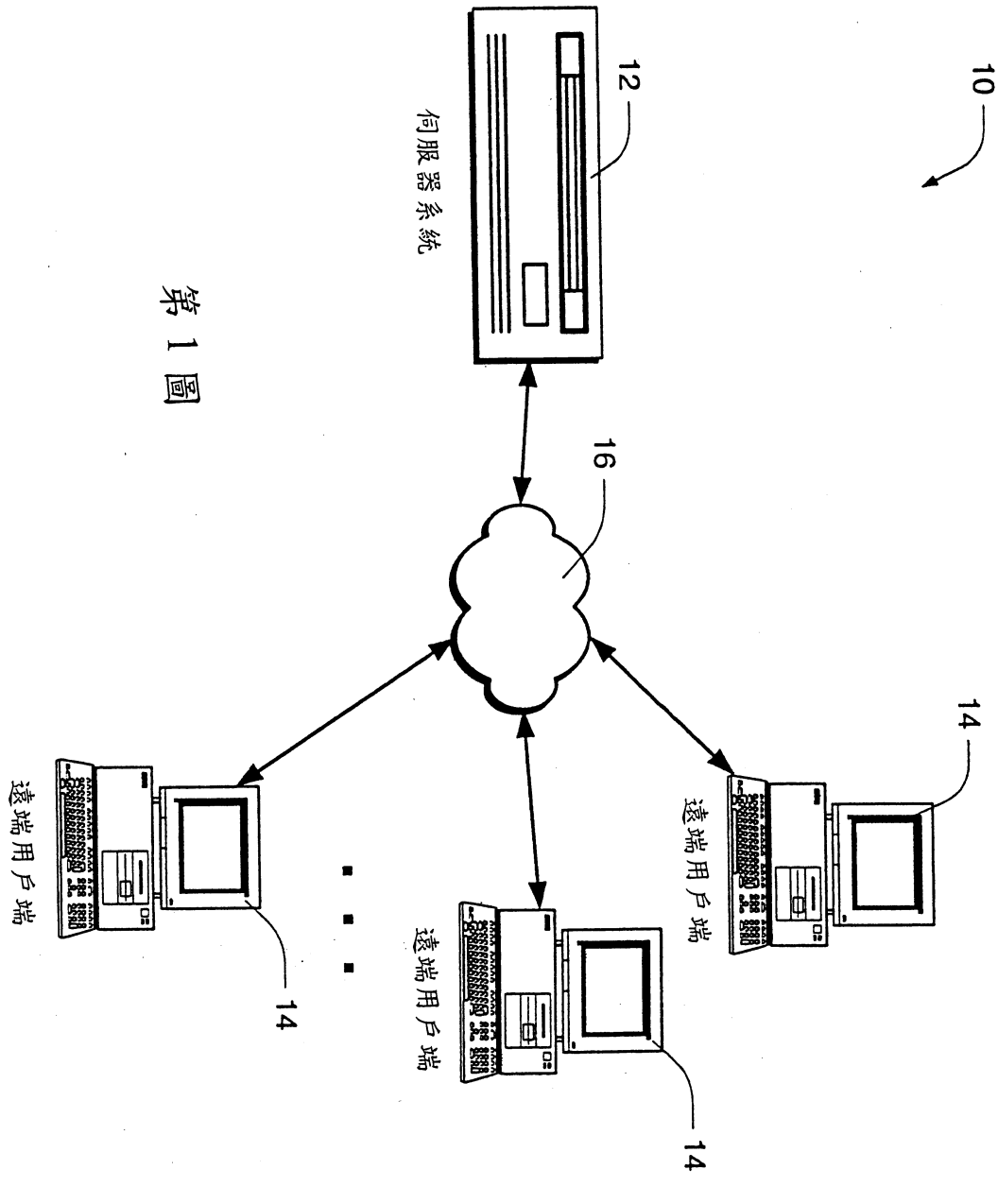
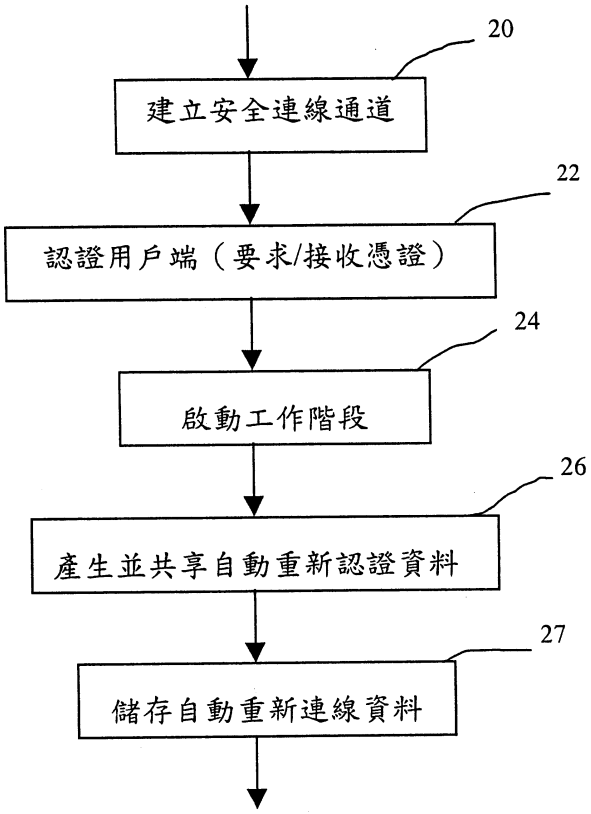
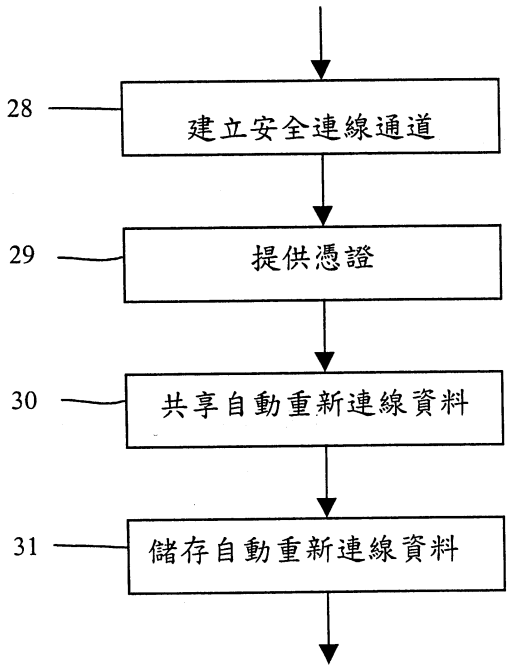


第 1 圖

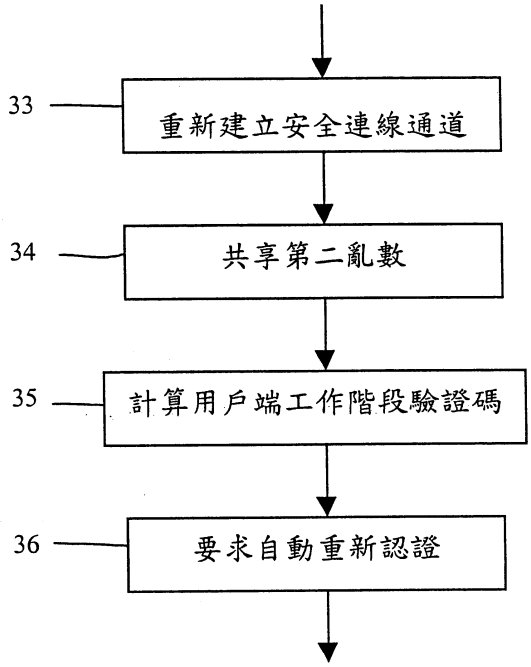
第 2 圖


20
建立安全連線通道
22
認證用戶端（要求/接收憑證）
24
啟動工作階段
26
產生並共享自動重新認證資料
27
儲存自動重新連線資料

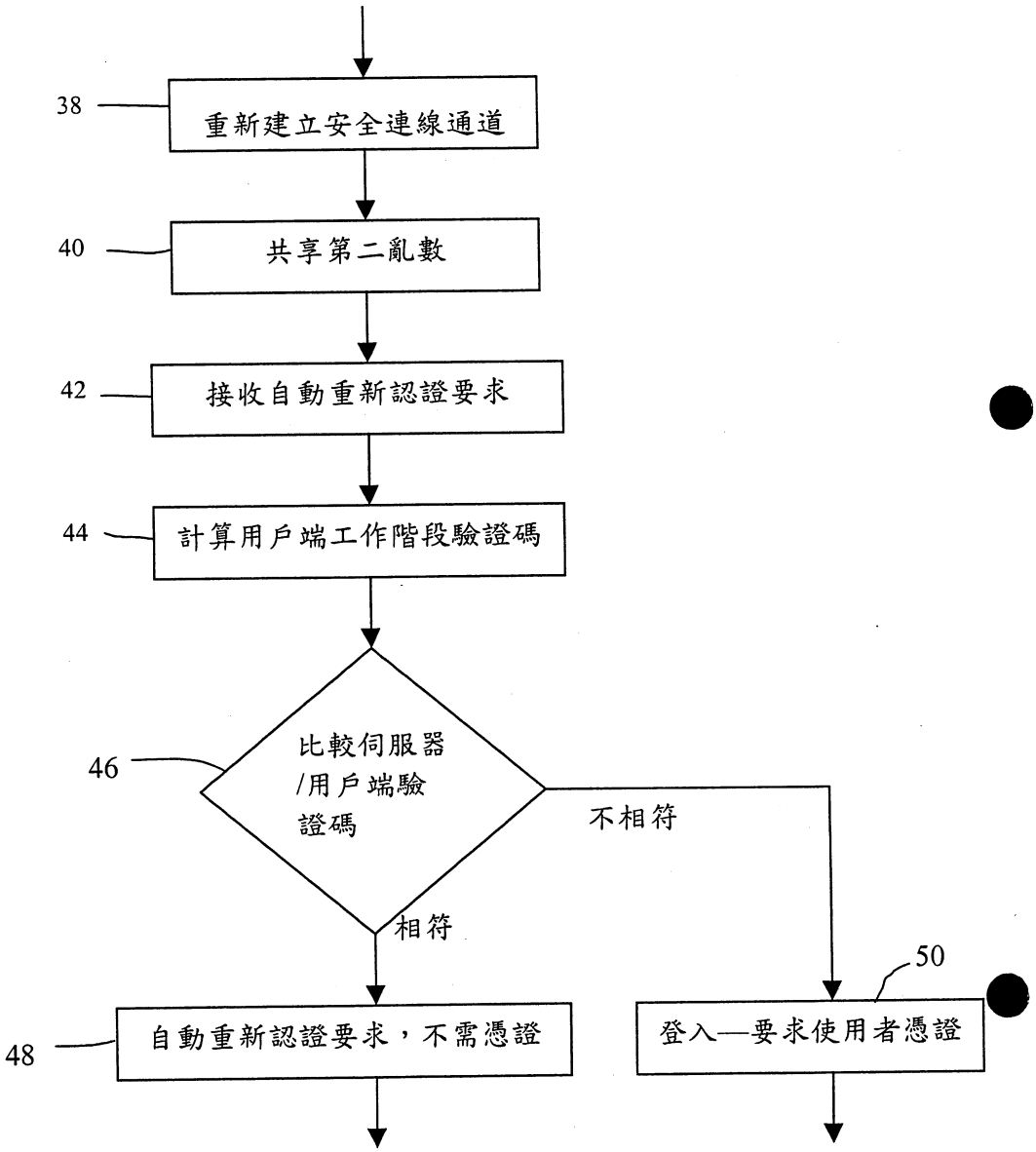
第 3 圖



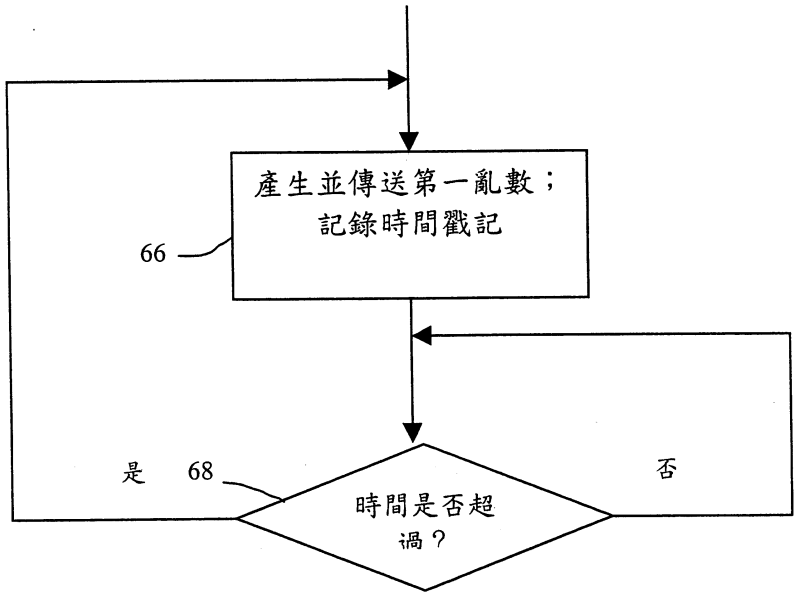
第 4 圖

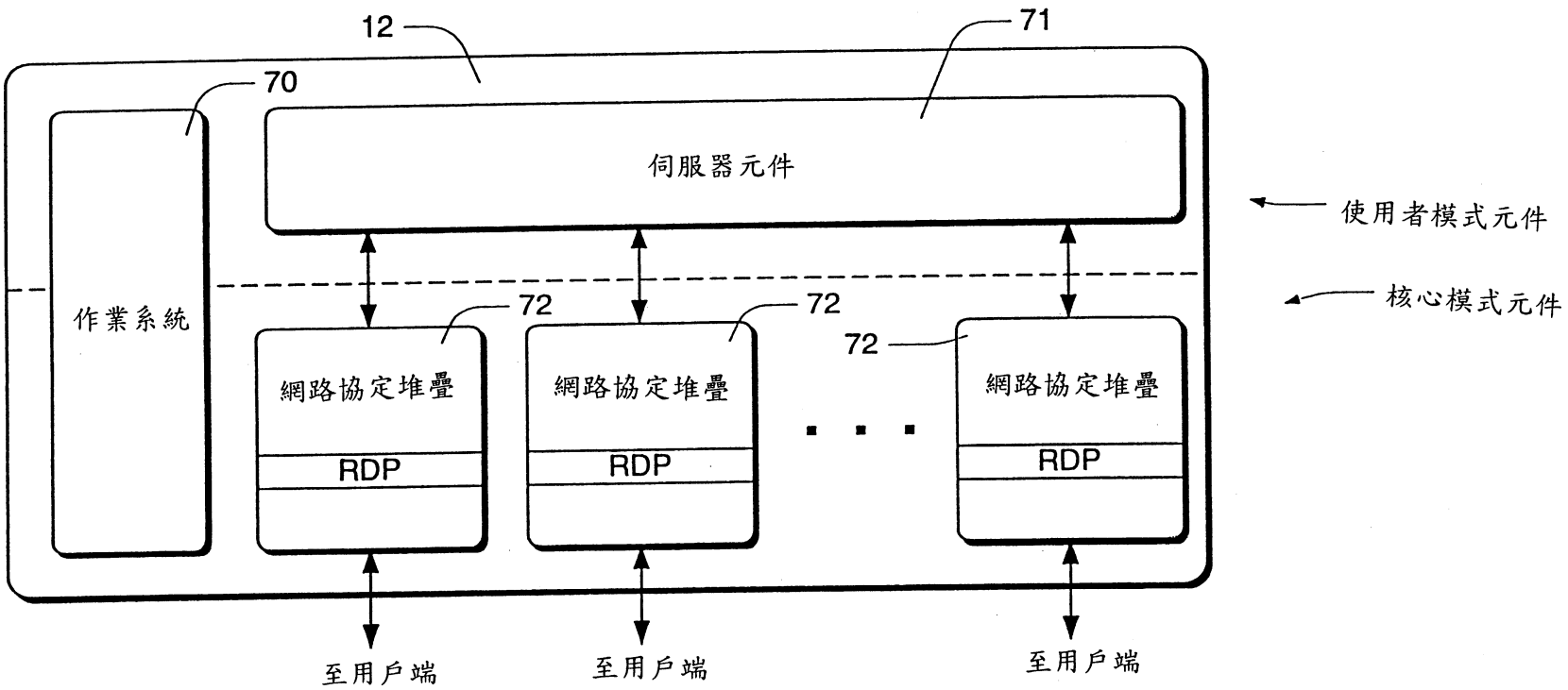


第 5 圖


38
重新建立安全連線通道
40
共享第二亂數
42
接收自動重新認證要求
44
計算用戶端工作階段驗證碼
46
比較伺服器/用戶端驗證碼
不相符
相符
50
登入—要求使用者憑證
48
自動重新認證要求，不需憑證

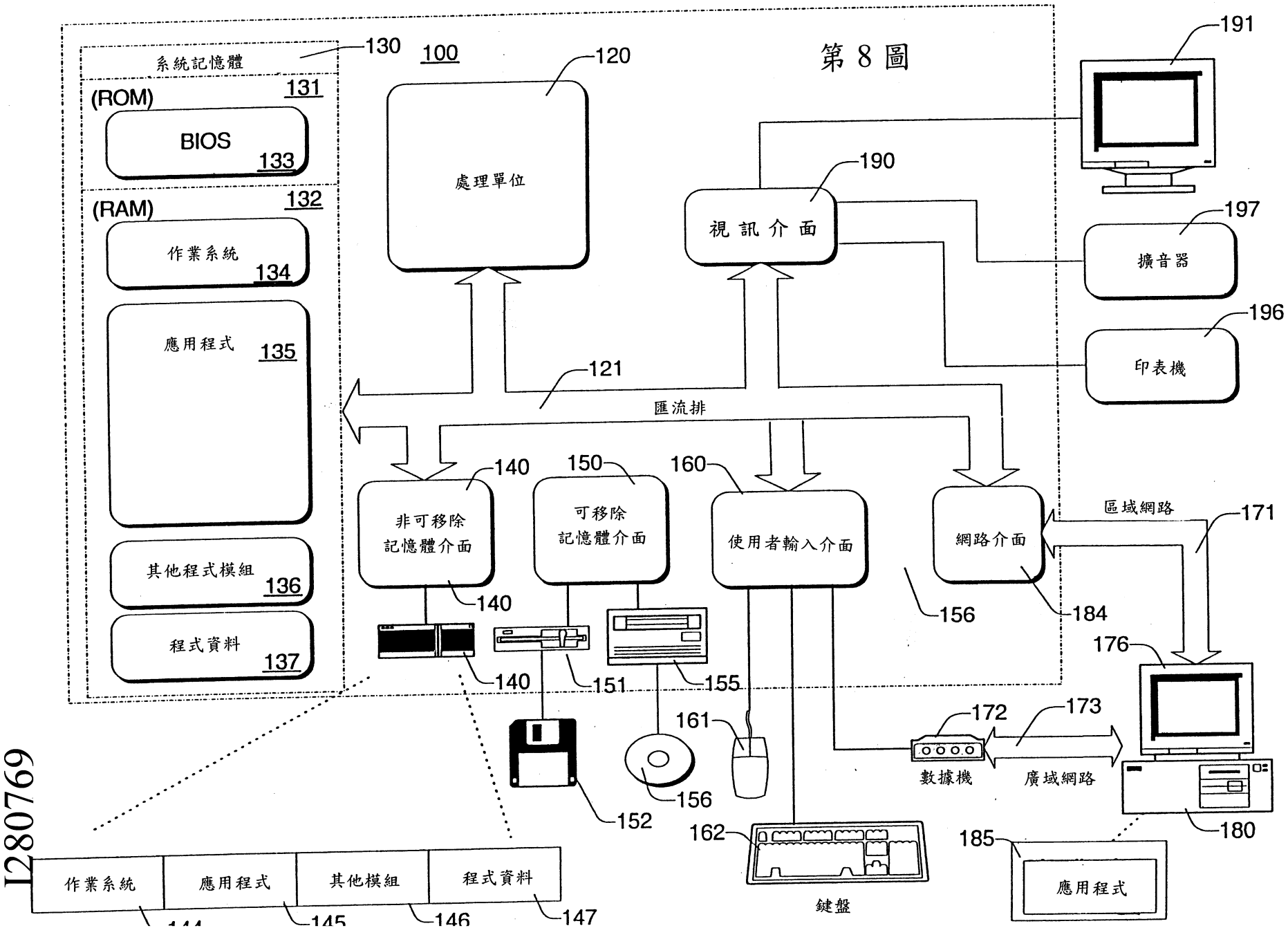
第 6 圖




12
71
70
伺服器元件
使用者模式元件
核心模式元件
作業系統
72
72
72
網路協定堆疊
網路協定堆疊
網路協定堆疊
RDP
RDP
RDP
至用戶端
至用戶端
至用戶端

第 7 圖

第 8 圖


系統記憶體
130
100
120
(ROM)
131
BIOS
133
(RAM)
132
作業系統
134
應用程式
135
其他程式模組
136
程式資料
137
處理單位
191
視訊介面
190
擴音器
197
印表機
196
121
匯流排
非可移除
記憶體介面
140
可移除
記憶體介面
150
使用者輸入介面
160
網路介面
區域網路
171
156
184
176
140
140
151
155
161
172
173
數據機
廣域網路
152
156
162
180
185
鍵盤
應用程式
作業系統
應用程式
其他模組
程式資料
144
145
146
147

公告本

第92104331號專利案96年1月修正 I280769

發明專利說明書

96 1 10 更正本

（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：92104331

※ 申請日期：2003 年 2 月 27 日　　※IPC 分類：H04L 9/32 (2006.01)

一、發明名稱：（中文/英文）

自動重新認證之系統、裝置及方法

SYSTEM, DEVICE AND METHOD OF AUTOMATIC RE-AUTHENTICATION

二、申 請 人：（共 1 人）

姓名或名稱：（中文/英文）

美商．微軟公司

Microsoft Corporation

代表人：（中文/英文）

丹尼爾 D.可萊斯

DANIEL D. CROUSE

住居所或營業所地址：（中文/英文）

美國華盛頓州列德蒙微軟路 1 號

One Microsoft Way, Building 8, Redmond, WA 98052-6399, U.S.A.

國　籍：（中文/英文）

美國/USA

三、發明人：（共 6 人）

姓　名：（中文/英文）

1.南定 Y. 阿都/NADIM Y. ABDO

2.亞當 J. 歐文頓/ADAM J. OVERTON

3.強森卡門斯/JASON GARMS

4.約翰 E.帕森斯二世/JOHN E. PARSONS JR.

5.艾文羅/ALVIN LOH

6.史考特 A. 費爾德/SCOTT A. FIELD

國　籍：(中文/英文)

1.加拿大/CANADA

2.美國/USA

3.美國/USA

4.美國/USA

5.加拿大/CANADA

6.英國/UK

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：

美國；2002 年 4 月 1 日；10/116,803

☐ 無主張專利法第二十七條第一項國際優先權：

☐ 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。

5.艾文羅/ALVIN LOH

6.史考特 A. 費爾德/SCOTT A. FIELD

國　籍：(中文/英文)

1.加拿大/CANADA

2.美國/USA

3.美國/USA

4.美國/USA

5.加拿大/CANADA

6.英國/UK

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：

美國；2002 年 4 月 1 日；10/116,803

☐ 無主張專利法第二十七條第一項國際優先權：

☐ 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。

九、發明說明

【發明所屬之技術領域】

本發明係關於在含有遠端終端機之系統內，使用者與工作階段之認證。

【先前技術】

Microsoft® Windows®伺服器作業系統的某些版本支援『終端機服務』。透過終端機服務，一伺服器系統可以將傳統的 Windows®桌面、與最新的 Windows®相關應用程式運送到位在遠端的桌上型運算裝置，也就是所稱的用戶端裝置或遠端終端機。該遠端終端機通常是一執行特定終端機模擬軟體之個人電腦。在此處所述的 Microsoft® Windows®環境下，該遠端終端機可執行特別為 Windows®終端機服務作業所設計的程式。

當一使用者在此環境下執行一應用程式時，其應用程式執行、資料處理、以及資料儲存，大多數或全部在伺服器上進行；只有例如鍵盤、滑鼠、顯示、與列印資訊是在伺服器與遠端終端機間來回傳送。

單一的伺服器系統可支援多重使用者以及相對應的使用者工作階段。每一位使用者登入後僅能看到其個人的工作階段，該工作階段完全由伺服器作業系統管理，且獨立於任何其他用戶端工作階段。

通常，伺服器系統與不同遠端終端機之間會透過某種網路進行連線。該網路可以是一種私用區域網路、一種私用或公

用廣域網路、或一種可供公眾存取的網路，如網際網路。對於原本未安全化的網路連線，可在伺服器系統與遠端終端機之間，利用不同形式的加密來確保隱私權與資料的完整性。在設計上，伺服器系統軟體與遠端終端機軟體皆可支援加密。

Microsoft® Windows®終端機服務利用遠端桌面協定（RDP，remote desktop protocol），這是一種展示服務協定，可以控制伺服器系統與遠端終端機之間的連線。RDP 利用本身在伺服器系統上的視訊驅動程式來轉譯顯示輸出，可將轉譯中的資訊建構至網路封包內，並透過網路將其傳送到用戶端裝置。用戶端接收到轉譯中的資料，並將之解譯成相對應的 Win32® GDI API 呼叫。同樣地，可將用戶端滑鼠與鍵盤的訊息自用戶端重新導向至伺服器。在伺服器上，RDP 利用本身的虛擬鍵盤與滑鼠驅動程式，來接收這些鍵盤與滑鼠事件。除了這些基本輸入/輸出功能之外，RDP 也可對多種其他功能提供支援，例如列印重新導向、剪貼對應、遠端控制項、以及網路負載平衡。此外，RDP 可進行資料壓縮、資料加密、以及登入與登出服務。典型的 RDP 連線是封裝或內嵌在 TCP/IP 協定內。

伺服器系統能夠執行數個不同的工作階段。每一個使用者工作階段通常會和一位使用者及遠端終端機建立關聯，即使同一個工作階段可能在不同時期和不同遠端終端機建立關聯。要啟動一使用者工作階段，該使用者需在特定用戶端裝置與伺服器系統間，建立一安全化連線。之後，該伺服器系統利用用戶端裝置的 I/O 能力來認證該使用者，這個過程稱為『登

入』處理程序。典型的認證過程會要求使用者憑證，通常其至少包含一使用者名稱與密碼。接收有效憑證後，伺服器系統會建立一工作階段並將此用戶端裝置連線至該工作階段。

在許多網路環境中，特別是在網際網路環境下，資料連線並不可靠，且可能容易遺失。在前述的終端機服務環境下，伺服器系統與用戶端裝置之間的資料連線遺失時，並不必然會中止關聯至該用戶端裝置的工作階段。該工作階段反而會在一段預先定義的時期內持續作用，且使用者可利用相同的用戶端裝置或一不同的用戶端裝置，重新登入該工作階段。此登入處理程序和初始登入處理程序相似，因為伺服器系統經由要求使用者憑證來認證使用者。然而，伺服器系統可辨識該使用者正關聯至一現存工作階段，並將使用者重新連線至該工作階段，而非建立一新工作階段。在某些系統中，用戶端裝置可能會保留一來自前一工作階段的工作階段識別碼，並在後續的登入處理程序中，提交該工作階段識別碼，以便重新連線至該工作階段。

【發明內容】

成功地以一伺服器系統認證一用戶端裝置後，用戶端裝置與伺服器系統可共享自動重新連線資料。當與該伺服器系統失去並重新建立連線之後，該用戶端會向伺服器傳送一自動重新認證要求。該自動重新認證要求包括一工作階段驗證碼，此驗證碼至少部分係基於該共享的自動重新連線資料。伺服器會查驗該工作階段驗證碼。若成功通過該驗證，伺服器會自動重

新認證該用戶端裝置。

【實施方式】

下列說明提出一用戶端/伺服器系統之特定具體實施例與其元件，該系統係併入了所附申請專利範圍中列舉之元件。為了符合法定要件，具體明確地描述了具體實施例。然而，該說明之用意並非限制本專利之範圍。更有甚者，發明人已仔細考量過該申請專利之發明可能還有其他具體實施之方法，可包含在現有或未來技術下，與本文件所述元件相似的不同元件或元件之組合。

第 1 圖顯示一終端機伺服器系統 10 之示範性具體實施例。系統 10 包括一伺服器電腦或系統 12 以及多個遠端終端機或用戶端裝置 14。遠端用戶端 14 透過一網路 16，和伺服器電腦 12 連線，該網路 16 可以是一區域網路、一廣域網路、一種可讓公眾存取的網路，如公用網際網路、或其他多種資料連線網路。或者是，一或多個遠端用戶端 14 可利用非網路之方式，和伺服器系統 12 連線，例如專用的或視需要撥號連線，或其他直接點對點資料連線之形式。

伺服器系統 10 與個別的用戶端電腦皆為傳統、一般的桌上型電腦或其他類型的電腦，但專門的電腦或其他有更特定目的之裝置也可用來執行這些元件的功能。關於適合執行所述功能之電腦，將在下文連同第 8 圖提出其一特定且詳細之實施例。

在所述之具體實施例中，伺服器系統 12 執行 Microsoft®

Windows®伺服器作業系統的一種版本，且包括如前所述之終端機伺服器功能，通常稱為『終端機服務』。如上述，應用程式在此環境下，於伺服器系統 12 上執行，而非在個別的用戶端裝置 14 上。然而，鍵盤、滑鼠、顯示、與列印資訊會在伺服器與遠端終端機之間來回傳送。這種責任的區分，對使用者大致上很清楚。對一位使用者而言，該應用程式表面上正由用戶端裝置所執行；使用者介面功能，包括圖形介面元件以及使用者輸入功能是在用戶端裝置上進行。在許多情況下，用戶端裝置會配有終端機模擬軟體，使這些功能和伺服器協調。

Microsoft® Windows®伺服器作業系統的終端機服務可和遠端終端機或用戶端裝置 14 執行多重伺服器工作階段，其中使用者應用程式主要在伺服器系統上執行，而使用者 I/O 主要在用戶端裝置上執行。『工作階段』一詞，一般係指一組變更中之狀態資訊，且其和一特定用戶端裝置結合。在一終端機伺服器環境下，例如此處所述之環境，此狀態資訊存在於伺服器系統 12 中，而非於個別的用戶端電腦 14 中。一特定用戶端電腦之工作階段或狀態資訊，和任何伺服器系統 12 代表用戶端電腦而正在執行中之應用程式有關。

必須指出，雖然本發明之係以 Microsoft® Windows®伺服器作業系統與其終端機服務元件加以說明，但亦可使用其他的執行方式。本發明可用於多種情況，其中當一伺服器需認證用戶端，以便允許該用戶端利用伺服器之服務。當伺服器/用戶端連線不可靠且可能中斷時，本發明特別有用。

第 2-5 圖顯示，連線失敗後，認證與自動重新認證，由

伺服器系統 12 與用戶端裝置 14 執行之相關動作。需注意，第 2-5 圖中顯示之該動作，係由伺服器系統 12 或一用戶端裝置 14 上所執行之軟體來執行。在所述之具體實施例中，該動作係整合於伺服器系統 12 上執行之終端機服務軟體中，或整合於用戶端裝置 14 上執行之終端機模擬軟體中。在其他具體實施例中，所述之動作可以整合於其他類型的軟體中。

第 2 圖顯示，由伺服器 12 為特定用戶端裝置建立一新的工作階段時，所執行之動作。一啟動動作 20 至少包含在伺服器系統 12 與用戶端裝置 14 之間，建立一安全化資料連線通道。在所述之具體實施例中，係利用 RDP（遠端桌面協定）與多種 RDP 所用之加密技術，來達成前述目標。RDP 利用由位於加州 Redwood City 的 RSA Data Security, Inc.發展的一種秘密金鑰加密文件法- RC4，將連線通道安全化。SSL（安全傳輸層）是另一種安全協定之實施例，可用來提供一安全化的連線通道。『安全化(secure)』一詞係指伺服器與用戶端之間的連線比較不容易受到可能的攔截或監聽。使用相對較未安全化之連線媒體，例如網際網路，通常是以加密來提供連線安全性。然而，當連線媒體本身已安全化時，可能就不必然要加密。

一後續的動作 22，可利用 RDP 在安全化連線通道中執行，該動作至少包含認證用戶端或一伺服器工作階段之用戶端裝置。在許多情形下，該動作至少包含一登入處理程序，其會要求或提醒位在用戶端裝置之使用者提供使用者憑證，如一使用者名稱與密碼，之後伺服器會接收並查驗該使用者憑證。

雖然使用者憑證通常至少包含一使用者名稱與密碼，也

可以利用其他類型的憑證。例如，可以要求使用者提供生物辨識資訊，如一指紋或視網膜掃瞄；提供一種硬體符記，如智慧卡或其他裝置；或提供其他形式的辨識。

在許多情況下，認證將受到伺服器系統 12 之控制，其可傳輸圖形提示，使其顯示於用戶端裝置 14，之後並可接收來自用戶端裝置 14 之使用者憑證。在某些情況下，在用戶端裝置 14 上執行的終端機模擬軟體可以具有特別的安全性功能，使其可和伺服器軟體聯合作業，以加強登入處理程序之安全性。

在成功的認證或登入處理程序之後，一動作 24 至少包含在伺服器系統 12 上，為提出要求之用戶端裝置啟動一工作階段。

進一步的動作 26，可在啟動用戶端之工作階段之前、之後、或同時執行，其至少包含產生並與用戶端裝置共享自動重新連線資料。該自動重新連線資料至少包含一工作階段識別碼，以及一第一亂數。在所述之具體實施例中，由伺服器系統 12 產生這些數值，並經由安全化連線通道將之送到用戶端裝置 14。工作階段識別碼是一種和用戶端上現行伺服器工作階段相關之數值，且對所有現正執行中之工作階段，都是獨特的。第一亂數為一 16-位元的數值，係利用加密文件安全化亂數產生器所產生，且可能包括虛擬亂數。

一動作 27 至少包含在伺服器儲存自動重新連線資料，以供後續使用。結合自動重新連線資料時，當伺服器工作階段產生自動重新連線資料時，伺服器亦可儲存一參照至該工作階

段。

第3圖說明用戶端裝置14替一特定用戶端裝置建立一新工作階段時，所執行之動作。大部分的情況下，這些動作與第4圖說明之動作相互對應。

一動作28至少包含在用戶端裝置14與伺服器系統12之間，利用前述之 RDP，要求並建立一安全化連線通道。後續的動作29至少包含在一登入處理程序中，向伺服器系統提供使用者憑證，使得伺服器系統12得以認證用戶端裝置14，並可啟動一和用戶端裝置14相關之伺服器工作階段。

一動作 30 至少包含和伺服器系統共享自動重新連線資料。如前所述，該自動重新連線資料至少包含一工作階段識別碼以及一第一亂數。在所述之具體實施例中，這兩種數值均接收自伺服器系統。在其他具體實施例中，這兩種數值之一或兩者可能是由用戶端裝置產生，並被送到伺服器。一動作31至少包含儲存用戶端裝置14上之自動重新連線資料。為了安全性目的，這些數值儲存在易變程式記憶體內較佳，而非儲存在用戶端裝置內之非易變檔案系統，這使得其他可能在用戶端裝置 14 上執行的應用程式程式不容易存取該自動重新連線資料。

第4圖說明和伺服器系統12失去並重新建立連線後，用戶端裝置14執行之動作。失去連線可能是因為一資料錯誤、逾時、連線媒體失敗、或多種不同事件之一。在許多情況下，此一失去連線是暫時的，而該使用者在短暫的延遲後，能夠使用戶端裝置14重新連線至伺服器系統12。重新連線通常需要

使用者執行一手動步驟。然而，重新連線處理程序可以自動化。明確地說，可以設計用戶端裝置 14 的終端機模擬軟體，在失去連線後，使其自動且重複地嘗試重新連線至伺服器系統。

不論重新連線處理程序是否自動化，最終結果是一動作 33 在用戶端裝置 14 與伺服器 12 之間，重新建立一安全化連線通道。一旦重新建立此一連線通道，一動作 34 會讓用戶端與伺服器共享一第二亂數。該第二亂數是和第一亂數不同的數值，然而其是由伺服器系統 12 以類似或相同於產生第一亂數的方法所產生。因此，該第二亂數為一 16 位元的數值，由用戶端裝置 14 自伺服器系統 12 接收。

其後，一動作 35 至少包含在用戶端裝置上，由至少自動重新連線資料之一部分，計算或衍生一用戶端工作階段驗證碼。更明確地說，其至少包含在某種程度上至少利用第一亂數，且在某種程度上至少利用第二亂數，來衍生用戶端工作階段驗證碼。在所述之具體實施例中，工作階段驗證碼係由前述兩種亂碼之某些組合所得之單向雜湊(one-way hash)。例如，可將該兩種數值相加、相乘、或串連起來，之後再執行一單向雜湊，便可產生該工作階段驗證碼。HMAC（雜湊訊息身份認證代碼）是一種適當的單向雜湊函式之實施例。亦可使用其他雜湊函式。

一動作 36 至少包含由伺服器系統要求不需提供使用者憑證之自動重新認證。在所述之具體實施例中，該動作至少包含由用戶端裝置向伺服器系統傳送一自動重新認證要求。該自

動重新認證要求包括（a）工作階段ID（先前在動作32中接收者）以及（b）前一動作計算之工作階段驗證碼。若該要求成功，用戶端裝置便重新連線至原本之伺服器工作階段。需注意該用戶端裝置不需為了進行自動重新認證而儲存該使用者憑證。

第5圖說明當用戶端裝置14與伺服器系統12間失去連線後，伺服器系統12執行之動作。一動作38至少包含在用戶端裝置14與伺服器系統12之間，重新建立一安全化連線通道。欲達此一目的，在回應由用戶端啟動之連線時，可利用RDP之加密功能或其他加密技術。

之後的動作40至少包含在伺服器系統12與用戶端裝置14之間，產生並共享該第二亂數。在所述之具體實施例中，伺服器系統12利用與產生第一亂數近似或相同之方法，產生該第二亂數。在其他具體實施例中，用戶端裝置可能必須負責產生該第二亂數，並將之傳送至伺服器系統12。

一動作42至少包含自用戶端裝置14接收自動重新認證要求。如前所述，該自動重新認證要求包括（a）一工作階段ID以及（b）用戶端裝置14利用前述方法計算所得之一用戶端工作階段驗證碼。

一動作44至少包含計算或衍生一伺服器工作階段驗證碼。伺服器工作階段驗證碼之計算方式與用戶端工作階段驗證碼相同，皆是利用第一與第二亂數之單向雜湊。

一動作46至少包含比較用戶端工作階段驗證碼與伺服器工作階段驗證碼，以查驗該用戶端工作階段驗證碼。若二驗

證碼相符，該驗證成功且會執行一動作 48，其會根據在自動重新認證要求中其接收之工作階段 ID 所代表之工作階段，來自動重新認證提出要求之用戶端裝置—不會要求使用者憑證。一旦所要求之工作階段通過認證，用戶端裝置可重新連線至該工作階段，且可繼續正常之工作階段作業。若二驗證碼不相符，該驗證不成功且自動重新認證之要求就會被拒絕。在這種情況下，用戶端裝置不會重新連線至所要求之工作階段，並會啟動一較傳統的使用者登入處理程序 50—一般會要求使用者輸入他或她的使用者憑證。

每當一用戶端裝置欲重新認證某一特定工作階段時，便會重複第 2 圖之動作 26 與 27，以及第 3 圖之動作 30 與 31。也就是說，在每次重新認證成功後，會重新產生一第一亂數，並會再一次地在伺服器系統與用戶端裝置之間共享。這可以確保在同一時間內，只有一用戶端裝置能夠連線至特定工作階段。

有一選擇性功能，可在預定的時間間隔上，自動重新產生並再次共享至少部分的自動重新連線資料。明確地說，大約每一個小時，在伺服器系統 12 與用戶端裝置 14 之間，會重新產生並重新共享第一亂數。在伺服器與用戶端之間，一旦共享了該新產生的第一亂數，舊亂數便失效，而不能用來重新連線。

第 6 圖顯示該處理程序，或是定期改變自動重新連線資料的亂部分，並將之傳送至用戶端。一動作 66 至少包含產生並傳送該第一亂數至用戶端，並紀錄一時間戳記。一個後續的動作 68 至少包含比較該時間戳記與現在時間，以決定預定時

期（例如一小時）是否已經過。若時間已經過，執行迴圈會返回動作 66，產生一新亂數並將之傳送至用戶端，且記錄一新的時間戳記。若該時期尚未屆滿，便會重複進行區塊直到比較之結果為真實，此時會再次執行動作 66。

第 7 圖顯示在一電腦的作業系統中，伺服器系統 14 實作的若干細節。在此一具體實施例中，電腦有一作業系統 70，其可控管所謂的使用者與核心模式。程式或程式元件一般上是由這兩種這些模式其中之一來執行。核心模式一般是保留給對於電腦作業比較關鍵的較低層級之系統軟體元件。應用程式一般是在非核心使用者模式下的作業系統中執行，且可呼叫核心模式之元件，以便執行系統層級功能。傳統上，電腦的微處理器硬體可支援核心模式。

在所述之一終端機伺服器系統之具體實施例中，有一或多個使用者層級伺服器元件 71，其可管理使用者工作階段並執行和使用者工作階段相關之不同功能。此外，尚有多重協定堆疊或連線元件 72，其可在核心模式下執行，能在伺服器與個別用戶端之間，執行較低層級之連線功能。一般而言，對每一個工作階段以及相對應的用戶端裝置 14，會有一個單一的協定堆疊 72。在 RDP 協定與較低層協定（如 TCP、IP、UDP 等）下，該堆疊可管理連線。一般而言，藉由伺服器元件 71 向堆疊 72 進行功能呼叫，可建立伺服器元件 71 與多重協定堆疊 72 之間的連線。

在所述之具體實施例中，一特定工作階段之協定堆疊 72 需負責產生且傳送第一亂數至相關之用戶端裝置，以及負責在

時間間隔上重新產生且重新傳送第一亂數。明確地說，每當呼叫協定堆疊來執行伺服器/用戶端連線時，它必須確認胎預定的時間區間是否已經過，且當時間已經過時，要重新產生與重新傳送第一亂數。如此一來，不需由終端機伺服器元件 71 發起，就可以改變並重新傳送該亂數。利用此一技術，只有在預定時期經過後，且該協定堆疊在傳送或接收資料時，才會傳送一新亂數。

該架構之優點在於其可避免利用到一專用的使用者模式『微調』執行序，因為在時間區間上定期重新傳送第一亂數至用戶端時，可能必須利用該執行序。利用此種執行序極可能耗費電腦資源。因此，不利用該執行序是非常顯著的優點。

在自動重新連線處理程序中，由一新協定堆疊 72 來處理收到的一自動重新連線要求，並將之傳送到終端機伺服器元件 71.這個要求其中一部份，是由該終端機伺服器元件接收一工作階段 ID 以及一用戶端工作階段驗證碼。經由接收到之工作階段 ID 識別出現行工作階段後，為了找出與其相關的第一亂數，伺服器元件 71 可識別與連線失敗前的工作階段相關之協定堆疊 72，並可向該協定堆疊查詢在該工作階段中，最近一次和用戶端共享之第一亂數。之後伺服器元件利用該亂數計算伺服器工作階段驗證碼並查驗自用戶端接收之工作階段驗證碼。

上述之不同的元件與功能可由個別的電腦進行實作。第 8 圖顯示此種電腦之元件的典型實施例，以數字 100 表示之。第 8 圖中顯示之元件僅為實施例，而非用於限制本發明之功能

的範圍；本發明並不一定需要依賴第 8 圖中顯示之功能。

一般而言，可利用多種不同的一般用途或特定用途之運算系統組態。為人熟知且適用於本發明的運算系統、環境、和/或組態之實施例包括，但不限於，個人電腦、伺服器電腦、手提式或膝上型裝置、多處理器系統、以微處理器為基礎之系統、機上盒、可程式化之消費性電子產品、網路 PC、迷你電腦、主電腦、包括任何上述系統或裝置之分散式運算環境、以及其他相類似者。

在許多案例中，係以電腦可執行的指令來實現電腦的功能，例如電腦可執行之程式模組。一般而言，程式模組包括常式、程式、物件、元件、資料結構等可執行特定工作或實作特定抽象資料類型。這些工作也可以由經過連線網路連結之遠端處理裝置來執行。在分散式運算環境下，程式模組可以位在本機與遠端電腦儲存媒體內。

指令和/或程式模組可在多個時間儲存於多個電腦-可讀取之媒體，其可能是電腦的一部份或可供電腦讀取。程式一般分散在如軟式磁碟、CD-ROM、DVD、或某些形式之連線媒體（如一調變訊號）上。由這些媒體，可將之安裝或載入至一電腦之次要記憶體。執行時，至少會將其部分載入電腦之主電子記憶體。此處所述之本發明包括這些與其他多種類型的電腦可讀取之媒體，而此類媒體需含有可和微處理器或其他資料處理器共同實作前述步驟與動作之指令、程式、和/或模組。當根據前述之方法與技術來程式化電腦時，本發明亦包括該電腦本身。

為了說明之目的，此處將程式以及其他可執行的程式元件，如作業系統，描述為分離之區塊，然而必須理解，此類程式與元件在不同時間會位在電腦中不同的儲存元件內，且係由電腦之資料處理（們）器執行。

參照第 8 圖，電腦 100 之元件可以包括，但不限於，一處理單位 120、一系統記憶體 130、與一系統匯流排 121，其可將不同系統元件，包括系統記憶體，結合至處理單位 120。系統匯流排 121 可以是多種類型的匯流排結構之一，包括一記憶體匯流排或記憶體控制卡、一周邊匯流排、與利用多種匯流排架構之任一種的本機匯流排。做為實施例，且非限制，此類架構包括工業標準架構（ISA）匯流排、微通道架構（MCA）匯流排、增強型 ISA（EISAA）匯流排、視頻電子標準協會（VESA）本機匯流排、以及周邊元件連接介面（PCI）匯流排，亦稱為夾層匯流排。

典型的電腦 100 包括多種電腦可讀取之媒體。電腦可讀取之媒體可以是任何可用之媒體，其可供電腦 100 存取，且包括易變與非易變媒體，可移除與非可移除媒體。做為實施例，而非限制，電腦可讀取的媒體可能至少包含電腦儲存媒體與連線媒體。在任何儲存資訊之方法或技術中，例如電腦可讀取的指令、資料結構、程式模組、或其他資料，所使用的電腦儲存媒體包括易變與非易變，可移除與非可移除媒體。電腦儲存媒體包括，但不限於，RAM、ROM、EEPROM、快閃記憶體或其他記憶體技術、CD-ROM、數位多功能光碟（DVD）或其他光碟儲存，卡式磁帶、磁帶、磁碟儲存或其他磁性儲存裝置、或

任何其他可用來儲存所需資訊，且可供電腦 110 存取之媒體。典型的連線媒體為電腦可讀取的指令、資料結構、程式模組或其他調變資料訊號中之資料，例如一載波或其他傳輸機制且包括任何資訊傳遞媒體。『調變資料訊號』一詞係指一訊號含有一或多種特性集合，或其改變之方式可在訊號中編碼資訊。做為實施例，而非限制，連線媒體包括有線媒體，例如一有線網路或直接有線連線與無線媒體，例如聲波、RF、紅外線、與其他無線媒體。任何前述媒體的組合，亦屬於電腦可讀取媒體之範圍。

系統記憶體 130 包括易變和/或非易變記憶體形式之電腦儲存媒體，如唯讀記憶體（ROM）131 與隨機存取記憶體（RAM）132。一基本之輸入/輸出系統 133（BIOS），含有基本常式，可協助電腦 100 內之元件間資訊之傳輸，例如在啟動中，其通常儲存於 ROM 131 中。典型之 RAM 132 含有資料和/或程式模組，其可立刻工處理單位 120 存取，和/或正由處理單位 120 作業中。做為實施例，而非限制，第 8 圖說明作業系統 134、應用程式 135、其他程式模組 136、以及程式資料 137。

電腦 100 可能還包括其他可移除/非可移除，易變/非易變電腦儲存媒體。僅做為實施例，第 8 圖說明一硬碟機 141，其可讀取或寫入非可移除、非易變磁性媒體；一磁碟機 151，其可讀取或寫入一可移除、非易變磁碟 152；以及一光碟機 155，其可讀取或寫入一可移除、非易變光碟 156 例如一 CD ROM 或其他光學媒體。其他能夠運用在示範性作業環境中之可移除/非可移除、易變/非易變電腦儲存媒體包括，但不限

於，卡式磁帶、快閃記憶卡、數位多功能光碟、數位視訊帶、固態 RAM、固態 ROM、及其他相似者。硬碟機 141 一般會經由一非可移除記憶體介面和系統匯流排 121 連接，例如介面 140；而磁碟機 151 與光碟機 155 一般會經由一可移除記憶體介面和系統匯流排 121 連接，例如介面 150。

第 8 圖中說明之前述磁碟機及其他相關的電腦儲存媒體，使得電腦 100 能儲存電腦可讀取的指令、資料結構、程式模組、與其他資料。舉例而言，在第 8 圖中，以儲存作業系統 144、應用程式程式 145、其他程式模組 146、與程式資料 147，來說明硬碟機 141。需注意這些元件可以相同或不同於作業系統 134、應用程式程式 135、其他程式模組 136、與程式資料 137。此處，以不同的數字代表作業系統 144、應用程式程式 145、其他程式模組 146、與程式資料 147，以便至少能夠說明其為不同的複本。一使用者可以利用輸入裝置，如一鍵盤 162 與指向裝置 161（一般稱為一滑鼠、軌跡球、或觸控板），將指令與資訊輸入電腦 100。其他輸入裝置（未顯示）可能包括一麥克風、搖桿、遊戲控制器、衛星接收器、掃描器、或其他類似者。這些與其他輸入裝置通常經由一與系統匯流排結合之使用者輸入介面 160 連接至處理單位 120，但也可能由其他介面與匯流排結構連接，如一平行連接埠、遊戲連接埠、或一通用序列匯流排（USE）。一監視器 191 或其他類型之顯示裝置可經由一介面連接至系統匯流排 121，例如一視訊介面 190。除了監視器之外，電腦亦可包括其他周邊輸出裝置，如擴音器 197 與印表機 196，其可經由輸出周邊介面 195 連接。

經由邏輯連結連線至一或多個遠端電腦後，如一遠端電腦 180，電腦可於一網路環境下作業。遠端電腦可能包括一個人電腦、一伺服器、一路由器、一網路 PC、一對等裝置或其他常見網路節點、且一般包括多種或全部前述與電腦 100 相關之元件，雖然第 8 圖僅說明一記憶體儲存裝置 181。第 8 圖中描述的邏輯連結包括一區域網路（LAN）171 以及一廣域網路（WAN）173，但也可能包括其他網路。例如，在辦公室內、企業內電腦網路、intranet、以及網際網路中，常見此種網路環境。

當運用在 LAN 網路環境內，經由一網路介面或介面卡 170，可將電腦 100 連線至 LAN 171。當運用在 WAN 網路環境下，電腦 100 一般包括一數據機 172，或其他可在 WAN 173 上建立連線之方法，例如網際網路。數據機 172，可以內建或外接，可經由使用者輸入介面 160 或其他合適的機制，連接至系統匯流排 121。在一網路環境下，所描述之與電腦 100 相關之程式模組，或其一部份，可能儲存在遠端記憶體儲存裝置內。做為實施例，而非限制，第 8 圖說明位在記憶體裝置 181 上之遠端應用程式程式 185。必須瞭解所顯示之網路連線為示範性質，尚可利用其他在電腦間建立連線連結之方式。

雖然於前文中詳細敘述了特定實作動作以及具體實施例，這些細節乃是為了滿足法定揭露義務，而非意圖限制下列申請專利範圍之範圍。因此，本發明係由申請專利範圍來界定，而非受限於前述之特定功能所述之。更有甚者，以等價物原則適當的解釋時，凡屬於所附申請專利範圍之合適範圍內的

任何形式或修改，皆屬於本發明之申請專利範圍。

【圖式簡單說明】

第 1 圖為一用戶端/伺服器系統之區塊示意圖，該系統包含了下述之本發明元件。

第 2 至 6 圖為流程圖，其顯示第 1 圖所示之伺服器系統與用戶端裝置所執行之步驟。

第 7 圖為一區塊示意圖，其顯示第 1 圖中伺服器系統元件，在一電腦之使用者與核心模式下執行。

第 8 圖為一示範性電腦之區塊示意圖，其可被程式化以執行此處所述之功能。

【元件代表符號簡單說明】

12 伺服器系統　　14 遠端用戶端

20 建立安全連線通道

22 認證用戶端（要求/接收憑證）

24 起始工作階段

26 產生並共享自動重新認證資料

27 儲存自動重新連線資料

28 建立安全連線通道　　29 提供憑證

30 共享自動重新連線資料

31 儲存自動重新連線資料

33 重新建立安全連線通道

34 共享第二亂數

35 計算用戶端工作階段驗證碼

36 要求自動重新認證

38 重新建立安全連線通道

40 共享第二亂數

42 接收自動重新認證要求

44 計算用戶端工作階段驗證碼

46 比較伺服器/用戶端驗證碼

48 自動重新認證要求，不需憑證

50 登入—要求使用者憑證

66 產生並傳送第依亂數；記錄時間戳記

68 時間是否經過？

70 作業系統

71 伺服器元件

72 網路協定堆疊

120 處理單位

121 匯流排

130 系統記憶體

131 ROM

132 RAM

133 BIOS

134 作業系統

135 應用程式

136 其他程式模組

137 程式資料

140 非可移除記憶體介面

144 作業系統

145 應用程式

146 其他模組

147 程式資料

150 可移除記憶體介面

160 使用者輸入介面

162 鍵盤

171 區域網路

172 數據機

173 廣域網路

184 網路介面

185 應用程式

196 印表機

197 擴 音 器

五、中文發明摘要

成功地以一伺服器系統認證一用戶端裝置之後，該用戶端裝置與伺服器系統可共享自動重新連線資料。當與該伺服器系統失去連線並重新建立連線之後，該用戶端向伺服器傳送一自動重新認證要求。該自動重新認證要求包括一工作階段驗證碼，此驗證碼至少部分係基於該共享的自動重新連線資料。伺服器會驗證該工作階段驗證碼。若成功通過該驗證，伺服器會自動重新認證該用戶端裝置。

六、英文發明摘要

Upon successfully authenticating a client device with a server system, the client device and server system shares auto-reconnect data. Upon subsequently losing and re-establishing communications with the server system, the client sends an auto-authenticate request to the server. The auto-authenticate request includes a session verifier that is based at least in part on the shared auto-reconnect data. The server validates the session verifier. If the validation is successful, the server automatically re-authenticates the client device.

十、申請專利範圍

1. 一種伺服器系統，其係經編程以執行至少包括下列動作：

認證一特定伺服器工作階段之一用戶端裝置；

與用戶端裝置共享自動重新連線資料；

在與用戶端裝置失去連線後，自用戶端裝置接收一工作階段驗證碼，該驗證碼至少部分係由自動重新連線資料產生；

查驗該工作階段驗證碼；

成功地查驗該工作階段驗證碼後，自動重新認證該特定伺服器工作階段之該用戶端裝置。

2. 如申請專利範圍第 1 項所述之伺服器系統，其中該重新認證步驟係於不要求使用者憑證下的情況被執行。

3. 如申請專利範圍第 1 項所述之伺服器系統，其中該自動重新連線資料係經由一安全化資料連線通道執行傳送。

4. 如申請專利範圍第 1 項所述之伺服器系統，其中該自動重新連線資料至少包含一亂數。

5. 如申請專利範圍第 1 項所述之伺服器系統，其中該自動重新連線資料至少包含與該特定伺服器工作階段相關之一工作階段 ID 以及一亂數。

6. 如申請專利範圍第 1 項所述之伺服器系統，其中：

該自動重新連線資料至少包含與該特定伺服器工作階段相關之一工作階段 ID 以及一亂數；

該工作階段驗證碼至少部分來自該亂數；

該等動作更包含與用戶端裝置失去連線後，自該用戶端裝置接收該工作階段 ID。

7. 如申請專利範圍第 1 項所述之伺服器系統，其中：

該等動作更包含與該用戶端裝置失去連線後，與該用戶端裝置共享一亂數；且

該工作階段驗證碼至少部分由該共享亂數與該自動重新連線資料所衍生。

8. 如申請專利範圍第 1 項所述之伺服器系統，其中：

該等動作更包含與該用戶端裝置失去連線後，與該用戶端裝置共享一亂數；且

該工作階段驗證碼為一單向雜湊，其至少部分基於（a）該共享之亂數與（b）該自動重新連線資料。

9. 如申請專利範圍第 1 項所述之伺服器系統，其中：

該自動重新連線資料至少包含一第一亂數；

該等動作更包含與該用戶端裝置失去連線後，與該用戶端裝置共享一第二亂數；

該工作階段驗證碼至少部分來自該第一亂數與第二亂

數。

10. 如申請專利範圍第 1 項所述之伺服器系統，其中：

該自動重新連線資料至少包含一第一亂數；

該等動作更包含與該用戶端裝置失去連線後，與該用戶端裝置共享一第二亂數；

該工作階段驗證碼至少包含一單向雜湊，其至少部分基於該第一與第二亂數。

11. 如申請專利範圍第 1 項所述之伺服器系統，其中該等動作更包含定期改變該自動重新連線資料之至少一部份，並至少將該改變之部分傳送至該用戶端裝置。

12. 如申請專利範圍第 1 項所述之伺服器系統，其中該自動重新連線資料至少包含一亂數，該等動作更包含定期改變該亂數，且將之傳送至該用戶端裝置。

13. 如申請專利範圍第 1 項所述之伺服器系統，其中查驗該工作階段驗證碼至少包含於伺服器系統計算該工作階段驗證碼，並比較該經計算之工作階段驗證碼與接收到之工作階段驗證碼。

14. 如申請專利範圍第 1 項所述之伺服器系統，更包含：

一作業系統；

一或多種連線程式元件，其可於該作業系統下之一核心模式內執行；

一或多種伺服器程式元件，其可於該作業系統下之一非核心模式內執行，以便實作伺服器工作階段；

其中該連線程式元件可於不啟動伺服器程式元件的情況下，定期將該自動重新連線資料之至少一部分，重新傳送至用戶端裝置。

15. 如申請專利範圍第 1 項所述之伺服器系統，更包含：

一作業系統；

一或多種連線程式元件，其可於該作業系統之核心模式下執行；

一或多種伺服器程式元件，其可於該作業系統下之一非核心模式內執行，以便實作伺服器工作階段；

其中該連線程式元件可於不啟動伺服器程式元件的情況下，定期改變並重新傳送該自動連線資料之至少一部分。

16. 如申請專利範圍第 1 項所述之伺服器系統，至少更包含：

一作業系統；

一或多種連線程式元件，其可於該作業系統之核心模式下執行；

一或多種伺服器程式元件，其可於該作業系統下之一非核心模式內執行，以便實作伺服器工作階段；

其中當與用戶端裝置連線中時，該連線程式元件（a）確認並決定，自從傳送該自動重新連線資料之至少一部份後，是否已經過一預定時期，以及（b）當該預定時間已超過，於不啟動伺服器程式元件的情況下，改變並重新傳送該自動重新連線資料之至少一部分。

17. 如申請專利範圍第 1 項所述之伺服器系統，其中：

不要求使用者憑證，便執行該重新認證；

該自動重新連線資料至少包含與該特定伺服器工作階段相關之一工作階段 ID 以及一第一亂數；

經由一安全化資料連線通道執行傳送該自動重新連線資料；

該等動作更包含，在與用戶端裝置失去連線後：

自該用戶端裝置接收該工作階段 ID；且

與該用戶端裝置共享一第二亂數；

該工作階段驗證碼至少部分來自該第一亂數與第二亂數；且

查驗該工作階段驗證碼，其至少包含於伺服器計算該工作階段驗證碼，並比較計算後之工作階段驗證碼與接收之工作階段驗證碼。

18. 一種終端機伺服器系統，其係被編程以執行至少包括下列動作：

與遠端終端機共同執行多重伺服器工作階段，其中使

用者應用程式主要在終端機伺服器系統上執行，而使用者I/O則經由遠端終端機執行；

要求使用者憑證，以便認證一特定遠端終端機之一特定伺服器工作階段；

經由一安全化連線通道，和該特定遠端終端機共享自動重新連線資料，該自動重新連線資料至少包含一第一亂數；

當連線失敗後，與特定遠端終端機重新建立連線；

重新建立連線後，與該特定遠端終端機共享一第二亂數；

自該特定遠端終端機接收一工作階段驗證碼，其至少部分來自該第一與第二亂數；

查驗該工作階段驗證碼；

成功地查驗該工作階段驗證碼後，自動重新認證該特定伺服器工作階段之該特定遠端終端機，不需再次要求使用者憑證。

19. 如申請專利範圍第18項所述之伺服器系統，其中：

該自動重新連線資料更包含與該特定伺服器工作階段相關之一工作階段ID；且

該等動作更包含，於重新建立連線後，自該特定遠端終端機接收該工作階段ID。

20. 如申請專利範圍第 18 項所述之伺服器系統，其中該工作

階段驗證碼為一單向雜湊，其至少部分基於該第一亂數。

21. 如申請專利範圍第 18 項所述之伺服器系統，該等動作更包含：

於重新建立連線後，與該特定遠端終端機共享一第二亂數；

其中該工作階段驗證碼為一單向雜湊，其至少部分基於該第一亂數與第二亂數。

22. 如申請專利範圍第 18 項所述之伺服器系統，其中該等動作更包含定期改變該第一亂數並將之重新傳送至該特定遠端終端機。

23. 如申請專利範圍第 18 項所述之伺服器系統，其中查驗該工作階段驗證碼至少包含於該終端機伺服器系統計算該工作階段驗證碼，並比較該計算過之工作階段驗證碼與接收之工作階段驗證碼。

24. 如申請專利範圍第 18 項所述之伺服器系統，更包含：

一作業系統；

一或多種連線程式元件，其可於該作業系統之核心模式下執行；

一或多種伺服器程式元件，其可於該作業系統下之一非核心模式內執行，以便實作伺服器工作階段；

其中該連線程式元件可於不啟動伺服器程式元件的情況下，定期改變該第一亂數，並將之重新傳送至該特定遠端終端機。

25. 如申請專利範圍第 18 項所述之伺服器系統，更包含：

一作業系統；

一或多種連線程式元件，其可於該作業系統之核心模式下執行；

一或多種伺服器程式元件，其可於該作業系統下之一非核心模式內執行，以便實作伺服器工作階段；

其中當與特定遠端終端機連線中時，該連線程式元件(a)確認並決定自從傳送該自動重新連線資料之至少一部份後是否已經過一預定時期，以及（b）當預定時間已經過，於不啟動伺服器程式元件的情況下，改變該第一亂數，並將之重新傳送至該特定遠端終端機。

26. 一種用戶端裝置，其係被編程以執行至少包括下列動作：

向一伺服器系統提供使用者憑證，使該伺服器系統能夠認證該用戶端裝置；

於一伺服器系統上啟動一伺服器工作階段，該伺服器工作階段係與該用戶端裝置相關；

與該伺服器系統共享自動重新連線資料，該自動重新連線資料至少包含一工作階段 ID 和一第一亂數；

自該第一亂數之至少一部份衍生一工作階段驗證碼；

與該伺服器系統失去連線並重新建立連線後，要求伺服器系統進行自動重新認證，且不需提供使用者憑證，其中該要求至少包含傳送該工作階段驗證碼至該伺服器系統。

27. 如申請專利範圍第 26 項所述之用戶端裝置，其中：

該等動作更包含與該伺服器系統失去連線後，與該伺服器系統共享一第二亂數；

由第一與第二亂數兩者之至少一部份，衍生該工作階段驗證碼。

28. 如申請專利範圍第 26 項所述之用戶端裝置，其中該動作更包含定期與該伺服器系統共享一已改變之第一亂數。

29. 如申請專利範圍第 26 項所述之用戶端裝置，其中該自動重新連線資料係接收自該伺服器系統。

30. 如申請專利範圍第 26 項所述之用戶端裝置，其中該要求更包含傳送一工作階段 ID 至該伺服器系統。

31. 一種用於在一用戶端裝置與一伺服器系統之間自動重新認證的方法，其至少包含：

在該用戶端裝置與該伺服器系統之間建立資料連線；

認證一特定伺服器工作階段之該用戶端裝置；

在該用戶端裝置與該伺服器系統之間，共享自動重新連線資料；

於該用戶端裝置，由該自動重新連線資料之至少一部份，衍生一用戶端工作階段驗證碼；

於連線失敗後，在該用戶端裝置與該伺服器系統之間重新建立資料連線；

重新建立資料連線後，自該用戶端裝置向該伺服器系統提供該用戶端工作階段驗證碼；

於該伺服器系統，由該自動重新連線資料之至少一部份，衍生一伺服器工作階段驗證碼；

比較該用戶端工作階段驗證碼與伺服器工作階段驗證碼，以查驗該用戶端工作階段驗證碼；

成功地查驗該工作階段驗證碼後，自動重新認證該特定伺服器工作階段之該用戶端裝置。

32. 如申請專利範圍第 31 項所述之方法，其中執行該重新認證時，不需要求使用者憑證。

33. 如申請專利範圍第 31 項所述之方法，其中該自動重新連線資料至少包含一亂數。

34. 如申請專利範圍第 31 項所述之方法，其中該自動重新連線資料至少包含與該特定伺服器工作階段相關之一工作階段 ID 以及一亂數。

35. 如申請專利範圍第 31 項所述之方法，其更包含：

重新建立資料連線後，在該用戶端裝置與該伺服器系統之間，共享一亂數；且

其中該用戶端工作階段驗證碼與該伺服器工作階段驗證碼至少部分來自該共享之亂數與該自動重新連線資料。

36. 如申請專利範圍第 31 項所述之方法，其中：

該自動重新連線資料包括一第一亂數；

該方法更包含，重新建立資料連線後，在該用戶端裝置與該伺服器系統之間，共享一第二亂數；且

該用戶端工作階段驗證碼與伺服器工作階段驗證碼至少部分來自該第一與第二亂數。

37. 如申請專利範圍第 31 項所述之方法，其中：

該自動重新連線資料包括一第一亂數；

該方法更包含重新建立資料連線後，在該用戶端裝置與該伺服器系統之間共享一第二亂數；且

該用戶端工作階段驗證碼與伺服器工作階段驗證碼至少包含一單向雜湊，其至少部分基於該第一與第二亂數。

38. 如申請專利範圍第 31 項所述之方法，其中該等動作更包含定期改變該自動重新連線資料之至少一部份，並在該用戶端裝置與該伺服器系統之間，至少共享該改變之部分。

39. 如申請專利範圍第 31 項所述之方法，其中該自動重新連線資料至少包含一亂數，該動作更包含定期改變該亂數並將之共享在該用戶端裝置與該伺服器系統之間。

40. 如申請專利範圍第 31 項所述之方法，其至少更包含：

於一作業系統之核心模式下執行一或多種連線程式元件；

於一作業系統之非核心模式下執行一或多種伺服器程式元件，以便實作伺服器工作階段；

於不啟動伺服器程式元件的情況下，該連線程式元件定期改變並重新傳送該自動重新連線資料之至少一部分至該用戶端裝置。

41. 如申請專利範圍第 31 項所述之方法，其更包含：

於一作業系統之核心模式下執行一或多種連線程式元件；

於一作業系統之非核心模式下執行一或多種伺服器程式元件，以便實作伺服器工作階段；

當與該用戶端裝置連線時，該連線程式元件（a）確認並決定自從傳送該自動重新連線資料之至少一部份後，是否已經過一預定時期，以及（b）當該預定時間已經過，於不啟動伺服器程式元件的情況下，改變並重新傳送該自動重新連線資料之至少一部分。

42. 一種電腦可讀取的媒體，其係含有可供電腦執行之指令，該指令係能執行至少包含下列動作：

與一用戶端裝置建立連線；

經由該用戶端裝置要求使用者憑證，以認證一特定伺服器工作階段之該用戶端裝置；

與用戶端裝置共享自動重新連線資料，該自動重新連線資料至少包含一第一亂數；

連線失敗後，與該用戶端裝置重新建立連線；

自該特定用戶端裝置接收一工作階段驗證碼，其至少部分來自該第一亂數；

查驗該接收之工作階段驗證碼；

成功地查驗該工作階段驗證碼後，自動重新認證該特定伺服器工作階段之該特定用戶端裝置，而不需再次要求使用者憑證。

43. 如申請專利範圍第 42 項所述之電腦可讀取的媒體，其中：

該自動重新連線資料更包含與該特定伺服器工作階段相關之一工作階段 ID；且

該等動作更包含於重新建立連線後，自該用戶端裝置接收該工作階段 ID。

44. 如申請專利範圍第 42 項所述之電腦可讀取的媒體，其中該工作階段驗證碼為一單向雜湊，其至少部分基於該第一

亂數。

45. 如申請專利範圍第 42 項所述之電腦可讀取的媒體，該等動作更包含：

於重新建立連線後，與該用戶端裝置共享一第二亂數；

其中該工作階段驗證碼至少部分衍生自該第一與第二亂數。

46. 如申請專利範圍第 42 項所述之電腦可讀取的媒體，該等動作更包含：

於重新建立連線後，與該用戶端裝置共享一第二亂數；

其中該工作階段驗證碼為一單向雜湊，其至少部分基於該第一與第二亂數。

47. 如申請專利範圍第 42 項所述之電腦可讀取的媒體，其中該等動作更包含定期改變該第一亂數並將之重新傳送至該用戶端裝置。

48. 如申請專利範圍第 42 項所述之電腦可讀取的媒體，該等動作更包含：

於一作業系統之核心模式下執行一或多種連線程式元件；

於一作業系統之非核心模式下執行一或多種伺服器程式元件，以便實作伺服器工作階段；

該連線程式元件可於不啟動伺服器程式元件的情況下，定期改變該第一亂數，並將之重新傳送至該用戶端裝置。

49. 如申請專利範圍第 42 項所述之電腦可讀取的媒體，該等動作更包含：

於一作業系統之核心模式下執行一或多種連線程式元件；

於一作業系統之非核心模式下執行一或多種伺服器程式元件，以便實作伺服器工作階段；

當與用戶端裝置連線時，該連線程式元件（a）確認並決定自從傳送該自動重新連線資料之至少一部份後，是否已經過一預定時期，以及（b）當該預定時間已經過，於不啟動伺服器程式元件的情況下，改變該第一亂數，並將之重新傳送至該用戶端裝置。

50. 一種電腦可讀取的媒體，其含有可由一用戶端電腦執行之指令，該指令係可執行至少包含下列之動作：

向一伺服器系統提供使用者憑證，以認證該用戶端電腦與該伺服器系統；

於一伺服器系統上啟動一伺服器工作階段，該伺服器工作階段係與該用戶端電腦相關；

與該伺服器系統共享自動重新連線資料，該自動重新連線資料至少包含一工作階段 ID 與一第一亂數；

與該伺服器系統失去連線並重新建立連線之後，要求該伺服器系統進行自動重新認證，且不需提供使用者憑證，其中該要求至少包含：

與該伺服器系統共享一第二亂數；

自該第一與第二亂數之至少一部份，衍生一工作階段驗證碼；

傳送該工作階段驗證碼至該伺服器系統。

51. 如申請專利範圍第 50 項所述之電腦可讀取的媒體，其中該等動作更包含與該伺服器系統定期共享一改變之第一亂數。

52. 如申請專利範圍第 50 項所述之電腦可讀取的媒體，其中該自動重新連線資料係接收自該伺服器系統。

53. 如申請專利範圍第 50 項所述之電腦可讀取的媒體，其中該要求更包含傳送一工作階段 ID 至該伺服器系統。

七、（一）、本案指定代表圖為：第 7 圖

（二）、本代表圖之元件代表符號簡單說明：

12　伺服器電腦或系統

70　作業系統

71　使用者層級伺服器元件

72　多重協定堆疊或連線元件

八、本案若有化學式時，請揭示最能顯示發明特徵的化學式：