I429256

公告本

發明專利說明書

（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：96144323

※ 申請日期：2007 年 11 月 22 日

※IPC 分類：

H04L 9/32 (2006.01)

一、發明名稱：（中文/英文）

基於編碼證明之重新驗證的鑑定授權

AUTHENTICATION DELEGATION BASED ON RE-VERIFICATION OF CRYPTOGRAPHIC EVIDENCE

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）

艾苹那諾爾 D 巴特萊

EPPENAUER, D. BARTLEY

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.梅德文斯基吉納迪/MEDVINSKY, GENNADY

2.南思尼爾/NICE, NIR

3.雪倫湯摩/SHIRAN, TOMER

4.梯普利思概亞力山大/TEPLITSKY, ALEXANDER

5.黎區保羅 J./LEACH, PAUL

6.倪史丹帝約翰/NEYSTADT, JOHN

國　籍：(中文/英文)

1.美國/USA

2.以色列/ISRAEL

3.以色列/ISRAEL

4.以色列/ISRAEL

5.美國/USA

6.以色列/ISRAEL

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；2006 年 12 月 1 日；11/607,720

☐ 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。

五、中文發明摘要：

一種用於實體鏈內的授權認證之方法，其係依賴在閘道設備和使用者之間的至少一部分之 TLS 握手，其中使用者需要存取期望之伺服器。該方法然後依賴對 TLS 握手之記錄部分中的編碼證明之重新驗證，該記錄部分被轉送到下列之一：（1）期望存取之伺服器，其中該伺服器重新驗證該記錄部分以確認認證；或（2）第三方實體，其中該第三方實體確認認證並將身份證明提供給該閘道伺服器，該閘道伺服器然後使用該身份證明來作為使用者，以向該伺服器進行認證。

六、英文發明摘要：

The method of delegating authentication, within a chain of entities, relies upon a recording of at least a portion of a TLS handshake between a gateway device and user, in which the user needs access to a desired server. The method then relies upon re-verification of cryptographic evidence in the recorded portion of the TLS handshake, which is forwarded either (1) to the server to which access is desired, in which case the server re-verifies the recorded portion to confirm authentication, or, (2) to a third party entity, in which case the third party entity confirms authentication and provides credentials to the gateway server which then uses the credentials to authenticate to the server as the user.

102年8月30日修正替換頁

七、指定代表圖：

(一)、本案指定代表圖為：第(1)圖。

(二)、本代表圖之元件代表符號簡單說明：

10 客戶端/使用者電腦系統

20 閘道

30 Web伺服器

35 包含客戶端認證之TLS握手

40 KDC或憑證管理中心

65 經由UC認證

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】

本發明係相關於一種基於編碼證明之重新驗證的鑑定授權。

【先前技術】

一組織可具有共同向使用者提供某些服務之實體鏈。對例如資料、網頁、功能軟體操作等資源之存取需要限制於一組已知或授權的使用者。目前已經研發了各種存取控制機制，以防止未授權的使用者和惡意攻擊者存取電腦資源，該等存取控制機制包含用於認證試圖存取網站資源的使用者身份之機構。具體而言，由於身份偷竊攻擊（例如網路釣魚、網址嫁接）增多，所以雙因數認證（two-factor authentication）越來越普遍。

雙因數認證（T-FA）係需要兩種不同方式來建立身份和權限的任何認證協定。雙因數認證的通常實施將“您熟知的某些事物”（例如密碼或個人識別碼）用作因數之一，並將“您具有的某些事物”（例如信用卡和硬體記號（token））或“您自身的某些事物”（例如指紋或視網膜圖案）之一用作另一因數。例如，智慧卡係提供雙因數認證的方法之一。智慧卡係硬體記號的示例，並且通常包含能夠執行各種安全操作（例如對所具有資料執行編碼功能）的微處理器。智慧卡通常具有一或多個國際電信聯盟（ITU-T）X.509 憑證（certificate）（及其相關聯私鑰），該等憑證可用於需要基於憑證之認證的協定。SSL（安全

通訊端層）、TLS（傳輸層安全）及 Kerberos（具有 PKINIT，即“用於 Kerberos 中之初始認證的公鑰編碼”的縮寫）均係此等協定之示例。

為了在不需使用智慧卡的情況下使用憑證。許多設備（例如電腦，行動電話）能夠儲存並利用憑證（及其相關聯私鑰）。例如，為了同步化電子郵件和行事曆資訊，Windows Mobile 5.0 可使用憑證向一 Exchange 2003 SP2 伺服器進行認證（經由在 SSL 和 TLS 頂部運行之 Exchange ActiveSync 協定）。

防止一組織之網路的實體鏈遭受身份偷竊攻擊（包含，例如，網路邊緣上的閘道設備提供對位於該組織內部網路（企業內部互聯網）的 Web 伺服器的基於 Web 的存取）是很重要的。

將認證授權廣義地定義為客戶端向伺服器授權認證，或更具體地，使得可存取資源（或伺服器）之第三方認證服務（或閘道）能夠代表使用者（透過在本質上模擬使用者）進行認證。被存取的伺服器將基於使用者身份而非基於認證服務帳號做出其認證決定。

提供此先前技術以介紹以下發明內容和實施方式之簡要背景。此先前技術並非意欲輔助確定本發明的範圍，也並非意欲被視為將本發明僅限定為該等能夠解決以上提出的任一或所有缺點或問題之實施。

【發明內容】

當使用者期望存取實體鏈中之特定伺服器時，基於重

新驗證（re-verification）或編碼證明（cryptographic evidence）之認證授權係利用閘道設備和使用者之間的至少一部分的TLS握手之記錄。透過將該TLS握手之記錄部分轉送到下列之一：（1）期望之伺服器，其中該伺服器重新驗證該記錄部分以確認認證；或者（2）第三方實體，其中該第三方實體透過重新驗證該記錄部分來確認認證，並將使用者身份證明（credential）提供給該閘道，該閘道然後使用該身份證明作為使用者向該伺服器認證。在每種情況中，該伺服器和該第三方實體利用該TLS握手之記錄部分做出是否准許使用者存取之決定，而不涉及該使用者與該閘道設備之間的認證。

在不同的說明性示例中，編碼證明包含時間戳記，該時間戳記透過確保TLS握手係及時的（即“最新”）來提供對安全之附加量測。此外，在確認有效的TLS握手之後，第三方實體可被配置為發出臨時（即有時間限制的）使用者身份證明，以使得閘道能夠例如利用具有PKINIT之Kerberos代表使用者向期望之伺服器進行認證。

提供此發明內容以透過簡單形式介紹選擇之概念。在實施方式部分中進一步描述該等概念。除在此發明內容中描述的該等元件或步驟之外的元件和步驟係可能的，然而沒有元件或步驟係必需的。此發明內容並非意欲標識本發明之關鍵特徵或實質特徵，亦並非意欲用於輔助確定本發明之範圍。本發明並不侷限於解決在此說明書任一部分中記載之任一或所有缺點之實施。

【實施方式】

基於重新驗證或編碼證明之認證授權的說明性情況係客戶端/使用者透過閘道存取一或多個服務提供者的情況。然而，應強調此情況僅係說明性的，其他情況和環境也係適當的。例如，當 Web 伺服器需要作為使用者向後端應用或資料庫進行認證時，或可選擇地在存在實體鏈並在該鏈的實體之間需要認證的任何設置中，可使用該認證授權。

關於存取，閘道設備提供對使用者提交請求之 Web 伺服器的存取，該請求到達閘道然後最終到達內部 Web 伺服器。然而，為了判斷正在連接的使用者是否被允許存取期望之資源，閘道和 Web 伺服器二者通常都需要某些形式的認證。

如果閘道被配置為使用表單式認證（FBA），則其需要使用者將使用者名稱和密碼輸入登入表單中。然後使用者提交該表單，並且該閘道接收使用者的使用者名稱和密碼。然後閘道可使用這些身份證明來代表使用者向內部 Web 伺服器進行認證。此係很簡單並且可能的，因為閘道接收密碼然後可如其所希望地使用該密碼。然而，如果使用某些認證機制則此係不可能的。例如，如果使用者使用不提供密碼的認證機制來向閘道進行認證，則閘道不具有其可重新使用以代表使用者向內部 Web 伺服器進行認證之任何身份證明。

現今已經提出了一些用於此問題之解決方案。例如，

一方案涉及“受信任的第三方”。在此，預先配置該受信任的第三方以“信任”閘道代表所有使用者向所定義的Web伺服器（或統稱為服務）組進行認證。此技術可被實施為使得閘道（或前端伺服器）能夠代表客戶端請求與其他伺服器一起使用之票證（ticket）之協定。然後該受信任的第三方希望代表任一使用者向閘道提供服務票證，從而使得閘道然後能模擬任一使用者。

該受信任的第三方還可被配置為在特殊條件下提供服務票證。例如，在Kerberos協定中，客戶端經由服務票證向閘道進行認證，並且Kerberos約束授權提供一種方法，藉由該方法該受信任的第三方（密鑰分配中心）可被配置為強制實行此條件。在此情況下，閘道必須提供如下的證明：提出要求之使用者確實已向閘道進行了認證（經由服務票證），這對於增加系統之整體安全性很重要。例如，需要此證明之優點係一安全受到危及之閘道將不能夠代表使用者存取伺服器，無需使用者首先向閘道正確地進行認證。

雖然該等提議提供了處理認證而無需密碼之方法，但在某些情況下，可能期望實施不涉及密鑰分配中心（KDC）或其他受信任的第三方實體之認證授權模型。在此一模型中，閘道將代表使用者向內部Web伺服器進行認證而不與KDC進行任何通信。存在許多提供此類功能之方案。例如，可將某些產品安裝/配置在閘道上以及任意數目的Web伺服器上，使得一旦使用者向閘道進行認證，閘道就返回一內部Web伺服器信任之記號（在某些情況下一HTTP（超

文件傳輸協定）網路資料記錄檔（cookie））。與使用其他協定一樣，此模型之一問題係閘道係完全受信任實體，因此降低了系統的整體安全性。

本發明提供基於編碼證明之重新驗證的認證授權。閘道（或前端伺服器）提供對 Web 伺服器（或後端伺服器）之存取。客戶端/使用者使用包含客戶端認證之 TLS 握手向閘道進行認證。該 TLS 握手之記錄，或至少足夠證明該使用者向該閘道進行了認證之 TLS 握手之記錄，然後被提供給以下二者之一：Web 伺服器（其重新驗證該握手的有效性），或第三方實體（其在驗證該記錄之後將使用者身份信息提供給之後向 Web 伺服器進行認證之閘道）。

請參照附圖，其中類似標號指示類似元件，第 1 圖示出利用本認證授權之示例性網路架構。客戶端/使用者電腦系統 10 有效地耦合到閘道 20（也稱作認證伺服器），閘道 20 使得在客戶端/使用者 10 和 Web 伺服器 30（也稱作網路伺服器）的網路之間能夠通信。閘道 20 包含資料庫/目錄（未示出），該資料庫/目錄包含認證使用者所必需之資訊（可替代地，該閘道可經由網路與外部使用者資料庫/目錄通信）。回應於登入，客戶端/使用者 10 首先經由如標號 35 所指示的包含客戶端認證之 TLS 握手向閘道 20 進行認證。應注意在此有意提到客戶端認證，因為在 TLS 握手協定中客戶端認證係可選的。

TLS 協定經由互聯網提供通信隱私（privacy），並使得客戶端/伺服器應用能夠以被設計為防止偷聽、篡改或訊

息假冒之方式通信。TLS握手協定使得伺服器和客戶端能夠彼此認證並使得其能夠在應用協定發送或接收其第一字節之資料之前協商加密算法和編碼密鑰。

TLS的優點之一係其係與協定無關的應用。因此更高級協定可透明地位於TLS協定之頂部。TLS握手協定可被概括如下：使用者/客戶端發送客戶端問詢(hello)訊息，對於該客戶端問詢訊息，伺服器（第1圖中，閘道20）必須以伺服器問詢訊息進行回應，否則將出現嚴重錯誤並且連接將出現故障。客戶端問詢和伺服器問詢被用於建立客戶端和伺服器之間的安全增強性能。

第6圖係示出在典型TLS握手階段期間客戶端和伺服器之間的訊息交換之示意性訊息流示圖。在RFC2246，TLS協定，版本1.0中詳細描述了TLS協定，該協定之公開部分被透過引用併入本文中。客戶端/使用者以客戶端－伺服器的關係與閘道設備通信。

更具體地，如第6圖所示，實際密鑰交換使用至多四條訊息：伺服器憑證（certificate）、伺服器密鑰交換、客戶端憑證和客戶端密鑰交換。透過指定此等訊息之格式並定義該等訊息之使用以使得客戶端和伺服器能夠認同共享之秘密，可創建新的密鑰交換方法。在問詢訊息之後，如果需要認證，伺服器會發送其憑證。此外，如果需要（例如，如果其伺服器沒有憑證，或如果其憑證僅用於簽章），伺服器密鑰交換訊息可被發送。

如果伺服器被認證，則其可請求來自客戶端之憑證，

如果其對於所選擇的密碼組而言係正確的。伺服器然後發送伺服器 hello 完成訊息，指示握手的問詢訊息階段已完成。伺服器然後等待客戶端回應。如果伺服器已經發送了憑證請求訊息，則客戶端必須發送憑證訊息。客戶端密鑰交換訊息被發送，並且該訊息的內容將依賴於在客戶端 hello 和伺服器 hello 之間選擇的公鑰算法。如果客戶端藉由簽章能力已經發送了憑證，則發送數位有符號憑證驗證訊息以明確驗證該憑證。

請參照第 1 圖，在此說明性示例中，閘道 20 創建作為此握手的一部分被交換之資料的記錄（第 1 圖中由標號 45 指示並示出為 THR）。更具體而言，該記錄至少包含直到憑證確認訊息之資料，該記錄由 TLS 握手之所有先前訊息上之簽章（signature）組成，並證實客戶端/使用者 10 確實持有與憑證匹配之私鑰。

然後，該 TLS 握手記錄或 THR 被作為客戶端/使用者 10 向閘道 20 進行了認證之認證證明（即“證據”）直接提供給 Web 伺服器 30。

內部 Web 伺服器 30 不涉及客戶端/使用者 10 和閘道 20 之間的認證，然而，客戶端/使用者 10 和閘道 20 之間的認證之認證證明（即 THR）被提供給 Web 伺服器 30，用於 Web 伺服器 30 然後作出是否提供對期望資源之存取的決定。

應注意，僅當 TLS 握手包含憑證確認訊息時才可使用所提議之機制。當所有以下條件為真時不使用此訊息：

(1) TLS 握手不包含客戶端認證。

(2) 客戶端和閘道決定繼續前一 TLS 會話或複製現有會話（而非協商新的安全參數）。在此情況下，TLS 握手不包含憑證確認訊息（參見 RFC 2246 中 30－31 頁）。

(3) 客戶端憑證具有簽章能力（即除了那些包含固定 Diffie-Hellman 參數的所有憑證）。例如，密碼組 ECDH_ECDSA 和 ECDH_RSA（參見 RFC 4492）支援客戶端認證然而並不利用憑證確認訊息。

第 2 圖係當客戶端/使用者 10 試圖存取第 1 圖所示之示例性架構中的 Web 伺服器時，所執行的認證過程之說明性流程圖。當客戶端/使用者想得到 Web 伺服器資源並存取閘道 20（步驟 200）時，該過程開始。如果客戶端/使用者未登入 Web 伺服器，則在 Web 伺服器允許存取之前客戶端/使用者必須被認證。

然後，客戶端/使用者請求想得到的 Web 伺服器資源（步驟 210）。為了認證該客戶端/使用者，閘道 20 和客戶端/使用者 10 接著用上文中詳細描述的方式執行包含客戶端認證之 TLS 握手（步驟 220）（熟悉此項技術者將理解，閘道 20 可在客戶端/使用者請求想得到的資源之前，或在客戶端/使用者請求該資源之後立即認證客戶端/使用者 10）。該 TLS 握手的至少一部分之記錄被生成並被提供給被請求的 Web 伺服器（步驟 230）。

在接收該 THR 之後，Web 伺服器 30 驗證客戶端/使用者已經向閘道進行了認證（透過確認該 THR 中之憑證確認

訊息中客戶端/使用者的簽章，並且在某些實施例中，還透過確認該 THR 中之時間戳記（將在下文中討論））（步驟240）。在假設客戶端/使用者被授權存取該 Web 伺服器的前提下，如果該 THR 被驗證，則准許存取被請求的 Web 伺服器（步驟 250），而如果該 THR 不能夠被驗證，則拒絕存取（步驟 260）。

如果攻擊者能夠獲得 THR 並嘗試將其重新使用來模擬客戶端/使用者，則為了防止或至少減輕此等“重播攻擊”，可想到一些技術和機制。首先，假設伺服器及/或客戶端/使用者將與時間相關的資料（例如，時間戳記）嵌入其握手訊息中，服務提供者（例如內部 Web 伺服器）可檢查所接收的 THR 以確認其係“最新的（fresh）”。此方案通常需要閘道 20 和 Web 伺服器 30（或客戶端/使用者 10 和 Web 伺服器 30）具有同步的時鐘，然而熟悉此項技術者應理解存在多種可能的回避設計。

可替代地，閘道 20 可向服務提供者（Web 伺服器 30）請求一亂數（nonce），並將該亂數嵌入其作為 TLS 握手之一部分發送到客戶端/使用者 10 的訊息之一中。服務提供者接著可檢查所接收的 THR 以確保其包含其先前生成的並傳送到閘道 20 之亂數。

應注意在此等兩種可能性之任一種中，閘道 20（或客戶端/使用者 10）將某些資料嵌入 TLS 握手訊息中（再次，握手協定本質上係一系列協商資料傳輸會話之安全參數的有序訊息）。通常以如下方式之一來完成此資料之嵌入：

(1) 伺服器可將時間戳記或亂數放入伺服器問詢訊息中，作為此訊息的隨機欄位之一部分（握手協定之此方面的細節可在 RFC 2246 的 7.4.1.3 部分中找到）；

(2) 伺服器可將時間戳記或亂數放入伺服器問詢延展部分(extension)中（細節可在 RFC 3546 的 2.2 部分中找到）；

(3) 客戶端/使用者可將時間戳記放入客戶端問詢訊息中，作為此訊息的隨機欄位之一部分（握手協定之此方面的細節可在 RFC 2246 的 7.4.1.2 部分中找到）；

(4) 客戶端/使用者可將時間戳記放入客戶端"hello"延展部分中(細節可在 RFC 3546 的 2.1 部分中找到)。

最後，除了上述每種可替代之選擇外，為了確保相同的 THR 只被使用一次，服務提供者（Web 伺服器 30）能夠記住其接收的所有 THR。經由某些共享存儲器或通信機制，還可在服務提供者之間共享此記憶。

在另一說明性實施中，可使用"雙" TLS 握手以進一步防止攻擊者危及閘道或客戶端與閘道之間的通信信道之安全。在此情況下，客戶端/使用者 10 和閘道 20 執行第一 TLS 握手而不包含客戶端認證。當第一 TLS 握手成功完成時，客戶端/使用者 10 和閘道 20 執行包含客戶端認證之第二 TLS 握手。藉由客戶端/使用者 10 和閘道 20 從第一握

手中得到之交談金鑰(session key)將隨後將被用作證明（THR）之該第二握手加密以傳輸。THR因此被保護，因為其並非係未加密地（即透明地）被發送，並且即使攻擊者能夠危及閘道20之安全，獲得THR也將更加困難。

如上所述在第1圖中示出之實施例由客戶端/使用者10、閘道20和服務提供者（Web伺服器30）組成。在下文中將進一步詳細討論之在第3圖中示出的替代實施例利用第三方實體40。在此情況下，服務提供者（Web伺服器30）“信任”第三方實體40提供使用者的真實身份。此一第三方實體40可以係一Kerberos KDC（如在S4U2Self + S4U2Proxy中那樣）或一憑證管理中心（CA）。應注意雖然第三方實體40在第3圖中被示出為獨立實體，然而在某些配置中該第三方實體（KDC或CA）可駐存於與閘道20相同的機器上。

在進一步具體討論第3圖中所示之實施例之前，吾人將討論Kerberos協定，其涉及受信任的第三方（已知為KDC）之使用，用於協商客戶端與伺服器之間的共享交談金鑰並提供它們之間的相互認證。

Kerberos的根基（corner-stone）係票證（ticket）和認證憑據（Authenticator）。票證將對稱密鑰（票證交談金鑰－僅存在一密鑰，在兩端點之間共享）封裝在一意欲用於特定服務的信封（一公開訊息）中。利用在服務主體與該發行密鑰的KDC之間共享的對稱密鑰加密票證的內容。票證的加密部分除了別的項以外包含客戶端主體名

稱。認證憑據係一記錄，該記錄可被示出為利用相關聯票證中之票證交談金鑰最近產生的。請求該票證的客戶端知道該票證交談金鑰。認證憑據的內容被利用該相關聯票證交談金鑰加密。認證憑據之加密部分除了別的項以外包含時間戳記和客戶端主體名稱。

如第4圖所示，Kerberos（V5）協定由在客戶端405和KDC410之間以及在客戶端405與應用伺服器415之間交換的以下訊息組成：

認證服務（AS）交換

客戶端從Kerberos認證伺服器（AS）獲得一“初始”票證，該票證通常係一票證核准票證（TGT）。AS-REQ訊息420和AS-REP425訊息分別係客戶端和AS之間之請求和應答訊息。

票證核准服務（TGS）交換

客戶端隨後使用該TGT進行認證，並請求來自Kerberos票證核准伺服器（TGS）之用於特定服務的服務票證。TGS-REQ訊息430和TGS-REP435訊息分別係客戶端和TGS之間之請求和應答訊息。

客戶端/伺服器認證協定（AP）交換

客戶端然後透過AP-REQ訊息440作出請求，AP-REQ訊息440由服務票證和確認客戶端具有票證交談金鑰之認證憑據組成。伺服器可視情況透過AP-REP訊息445予以應答。AP交換通常協商特定會話之對稱密鑰。

通常AS和TGS被整合到也已知為KDC的單個設備

中。

在AS交換中，KDC應答除了別的項之外包含票證交談金鑰，該KDC應答被利用客戶端與KDC之間共享的密鑰（AS應答密鑰）加密。對於人類使用者而言，該AS應答密鑰通常係從客戶端密碼中獲得。因此，對於人類使用者而言，Kerberos協定之抗攻擊強度不會比他們的密碼強度更強。

為了幫助資料原始認證以及理想保密，使用X.509憑證形式的非對稱編碼（參見由Internet Society（"ISOC"）管理的"Request for Comments"文獻系列下的RFC 3280）係常見的。一已建立的公鑰基礎建設（PKI）提供可用於建立認證和安全通信之密鑰管理及密鑰分配機制。將公鑰編碼添加到Kerberos提供了Kerberos與公鑰協定之良好的相合性，消除了人類使用者管理強大密碼的負擔，並使得Kerberized應用能夠利用現有密鑰服務和身份管理之優點。

Kerberos TGT所提供的優點係客戶端僅暴露其長期（long-term）秘密一次。TGT及其相關聯交談金鑰然後可被用於任何後續的服務票證請求。一結果係所有進一步之認證與執行初始認證之方法無關。因此，初始認證提供了將公鑰編碼整合到Kerberos認證中之便利場合。此外，出於對性能的考慮，較佳地在初始交換之後使用對稱編碼。

RFC 4456所述之方法和資料格式係利用客戶端和KDC可使用公鑰和私鑰對在AS交換中相互認證並協商AS

應答密鑰（僅客戶端和KDC知道該密鑰），並加密由KDC發送的之AS-REP之方法和資料格式。

請參照第3圖，在完成TLS握手（如同參考第1圖所討論者，其可以係“雙”握手）之後，閘道20將THR45提供給第三方實體40。如在第1圖的情況下，再次地，“受信任實體”（在此情況下係第三方實體40）作出決定而不涉及客戶端/使用者10與閘道20之間的認證。更確切地，受信任實體依據THR來判斷其是否將使用者身份證明提供給閘道。

更具體地，在交換有效的TLS握手（即THR）時，第三方實體40將如標號55所指示的使用者身份證明（UC）之表單返回給閘道20。閘道20然後如標號65所指示地使用該UC向Web伺服器30進行認證。在KDC的情況下，使用者身份證明將係一Kerberos服務票證或以使用者10之名稱命名的TGT。在CA的情況下，使用者身份證明將係一以使用者名稱命名之憑證（通常具有較短壽命）。

第5圖係示出當客戶端/使用者請求存取包含一第三方實體之系統中之Web伺服器時所執行的認證過程之步驟之說明性流程圖。在此系統中，當客戶端/使用者10存取閘道20時該過程開始（步驟500）。客戶端/使用者10然後請求期望的Web伺服器30資源（步驟510）。如果客戶端/使用者10未登入Web伺服器，則在Web伺服器30允許存取之前客戶端/使用者10必須被認證。

客戶端/使用者10和閘道20然後以上文中詳細描述之

方式執行包含客戶端認證之TLS握手（步驟520）。該TLS握手之至少一部分之記錄（THR）被產生並被提供給第三方實體（“受信任實體”）40（步驟530）。

在接收到該THR之後，第三方實體40驗證使用者已經向閘道進行了認證（透過確認該THR中之憑證驗證訊息）（步驟540）。如果驗證該THR有效並且係最新的（步驟550），則使用者身份證明（例如在憑證管理中心的情況下一臨時憑證，或在KDC的情況下一Kerberos服務票證）被提供給閘道20（步驟560）。閘道20然後使用該使用者身份證明以作為實際客戶端/使用者向Web伺服器30進行認證（步驟570）。然而如果該THR不能被驗證為有效並且最新（在步驟550），則使用者身份證明不會被提供給閘道20，然後存取被拒絕（步驟555）。

假設客戶端/使用者被授權存取Web伺服器，如果使用者身份證明（例如客戶端憑證）被Web伺服器30認證，則准許客戶端/使用者存取所請求的Web伺服器（步驟580），而如果客戶端憑證不能被驗證，則存取通常被拒絕（步驟590）。

提供給閘道20的使用者身份證明由一服務票證（在基於KDC的配置中）或一臨時憑證（在基於CA的配置中）組成。因為基於KDC的配置十分類似於在上文中討論之Kerberos約束授權（S4U2Self + S4U2Proxy），所以不再進一步討論。作為替代，將討論基於CA（基於憑證管理中心）的配置。

在基於 CA 的配置中，一或多個 CA 被用於在被提供有效並且“最新的” THR 時發出一客戶端憑證。在此情況下，服務提供者（Web 伺服器 30）必須被配置為信任該 CA（此通常意味著該 CA 自身的憑證必須被安裝在服務提供者操作系統上之某一特定位置中）提供使用者之真實身份。

一旦給出以使用者名稱命名之客戶端憑證（以及相關聯的私鑰），閘道 20 然後就使用這些身份證明以作為實際使用者向服務提供者 30 進行認證。為了使用該憑證和私鑰來向服務提供者（即 Web 伺服器 30）進行認證，閘道 20 和服務提供者必須使用支援客戶端憑證之認證協定。兩種為吾人熟知之支援客戶端憑證之認證協定係：TLS（或 SSL）－如在上文中詳細討論的，TLS（或 SSL）握手可包含客戶端認證（基於憑證）；或 Kerberos（w/ PKINIT）－題為“Public Key Cryptography for Initial Authentication in Kerberos”的 PKINIT 機制（RFC 4556），其係用於使得 Kerberos 使能之客戶端能夠經由公鑰編碼（即經由憑證和相關聯私鑰）獲得 TGT 之 Kerberos 協定的協定擴展機制。更具體地，此等擴展提供利用預認證資料欄位中之非對稱密鑰簽章及/或加密算法將公鑰編碼整合到初始認證交換中之方法。

假設客戶端/使用者被授權存取 Web 伺服器，一旦身份證明（客戶端憑證）被 Web 伺服器 30 認證，就准許客戶端/使用者存取所請求的 Web 伺服器。當然，如果客戶

端憑證不能被驗證（或如果 Web 伺服器未被配置為信任該 CA），則使用者對 Web 伺服器的存取被拒絕。

為了更進一步防止攻擊者危及閘道 20 之安全，與在第 1 圖的實施例中一樣，在第 3 圖的實施例中可實施“雙” TLS 握手。

雖然在此已經以具體到結構特徵及/或方法論行為之語言描述了本發明，但仍應理解，在隨附申請專利範圍中定義的本發明並非必須被限定於上述具體特徵或行為。更確切地，上述具體特徵和行為係作為實施隨附申請專利範圍之示例形式被公開。

例如，遍及此文獻，我們提及由客戶端/使用者透過閘道存取服務提供者組成之實體鏈。然而，此僅係一種可能情形，並且僅出於方便而在全文中使用之。其他可能情形包含需要作為使用者向後端應用或資料庫進行認證之 Web 伺服器。本發明的創新方面適用於任何如下之實體鏈：即該鏈中之實體之間需要認證。鏈中可具有任意數目之實體，在此每個實體必須作為原始客戶端向該鏈之下一實體進行認證。

還應理解，當一元件被指示為回應於另一元件時，該等元件可係直接或間接地耦合。在此描述之連接實際上可以係邏輯的或物理的連接以實現元件之間之耦合或通信連接。除了其他方式，可將連接實施為軟體處理之間之交互式處理通信，或聯網電腦之間之交互機通信。

在此使用之文字“示例性”和“說明性”用於表示用

作示例、實例或說明。在此被描述為“示例性”或“說明性”之本發明的任何實施或方面並非必須被解釋為與其其他的實施或方面相比較佳或更好。

應理解，可想到除以上描述之具體實施例外的實施例而不會背離隨附申請專利範圍之精神和範圍，在此，以下的申請專利範圍意欲覆蓋本發明之範圍。

【圖式簡單說明】

第1圖係基於對TLS握手訊息的重新驗證之認證授權的說明性架構的簡化原理方塊圖；

第2圖係示出利用第1圖之示例性架構之認證處理步驟的說明性流程圖；

第3圖係其中由第三方實體提供使用者身份證明之認證授權的說明性架構的簡化原理方塊圖，該第三方實體接收TLS握手的至少一部分之記錄；

第4圖示出Kerberos（V5）協定中客戶端與密鑰分配中心之間的說明性訊息交換；以及

第5圖係示出利用第3圖之示例性架構之認證處理步驟的說明性流程圖。

第6圖係示出在典型TLS握手階段期間客戶端與伺服器之間的訊息交換之示意性訊息流程圖。

【主要元件符號說明】

10　客戶端/使用者電腦系統

20　閘道

30　Web伺服器

35 包含客戶端認證之 TLS 握手

40 KDC 或憑證管理中心

45 KDC 或憑證管理中心

55 經由 UC 認證

65 經由 UC 認證

405 客戶端

410 KDC

415 應用伺服器

420 AS-REQ 訊息

425 AS-REP 訊息

430 TGS-REQ 訊息

435 TGS-REP 訊息

440 AP-REQ 訊息

445 AP-REP 訊息

十、申請專利範圍：

1. 一種在一客戶端/使用者透過一閘道存取一服務提供者時在其間認證授權(authentication delegation)之方法，該方法包括以下步驟：

執行傳輸層安全(Transport Layer Security；TLS)握手之步驟，在該客戶端/使用者和該閘道之間執行一包含客戶端認證的 TLS 握手，該包含客戶端認證的 TLS 握手係由一協定所定義，該協定指定(specify)複數個訊息之一交換；

記錄步驟，記錄該 TLS 握手之至少一足夠部分的訊息，以指出該客戶端/使用者係被該閘道所認證，其中該至少足夠部分的訊息包含在該協定中所指定之訊息，且該至少足夠部分的訊息包含所有在該協定中所指定之訊息直到並包括一憑證確認訊息(certificate verify message)，其中該 TLS 握手之至少足夠部分的訊息係在該客戶端/使用者與該閘道間交換；以及

提供步驟，將該直到並包括該憑證確認訊息之所有訊息的記錄自該閘道提供至該服務提供者，其中所有已提供之訊息係經數位簽章(digitally signed)，且其中，

存取該服務提供者係基於在該客戶端/使用者與該閘道間交換之該 TLS 握手之至少足夠部分的訊息。

2. 如申請專利範圍第 1 項所述之方法，其中該服務提供者與該客戶端/使用者和該閘道之間的認證無關。

3. 如申請專利範圍第 1 項所述之方法，其中該提供步驟將該記錄直接從該閘道提供給該服務提供者。

4. 如申請專利範圍第 1 項所述之方法，更包括將時間戳記(timestamp)資料嵌入至該 TLS 握手中的訊息之步驟。

5. 如申請專利範圍第 4 項所述之方法，其中該客戶端/使用者嵌入該時間戳記資料。

6. 如申請專利範圍第 4 項所述之方法，其中該閘道嵌入該時間戳記資料。

7. 如申請專利範圍第 1 項所述之方法，更包括如下之步驟：將由該服務提供者所提供之一亂數(nonce)嵌入至由該閘道傳送到該客戶端/使用者之一訊息中，以作為該 TLS 握手的一部分。

8. 如申請專利範圍第 1 項所述之方法，其中該服務提供者保存對所有已接收的記錄之一記憶，並確認一相同記錄僅被使用一次。

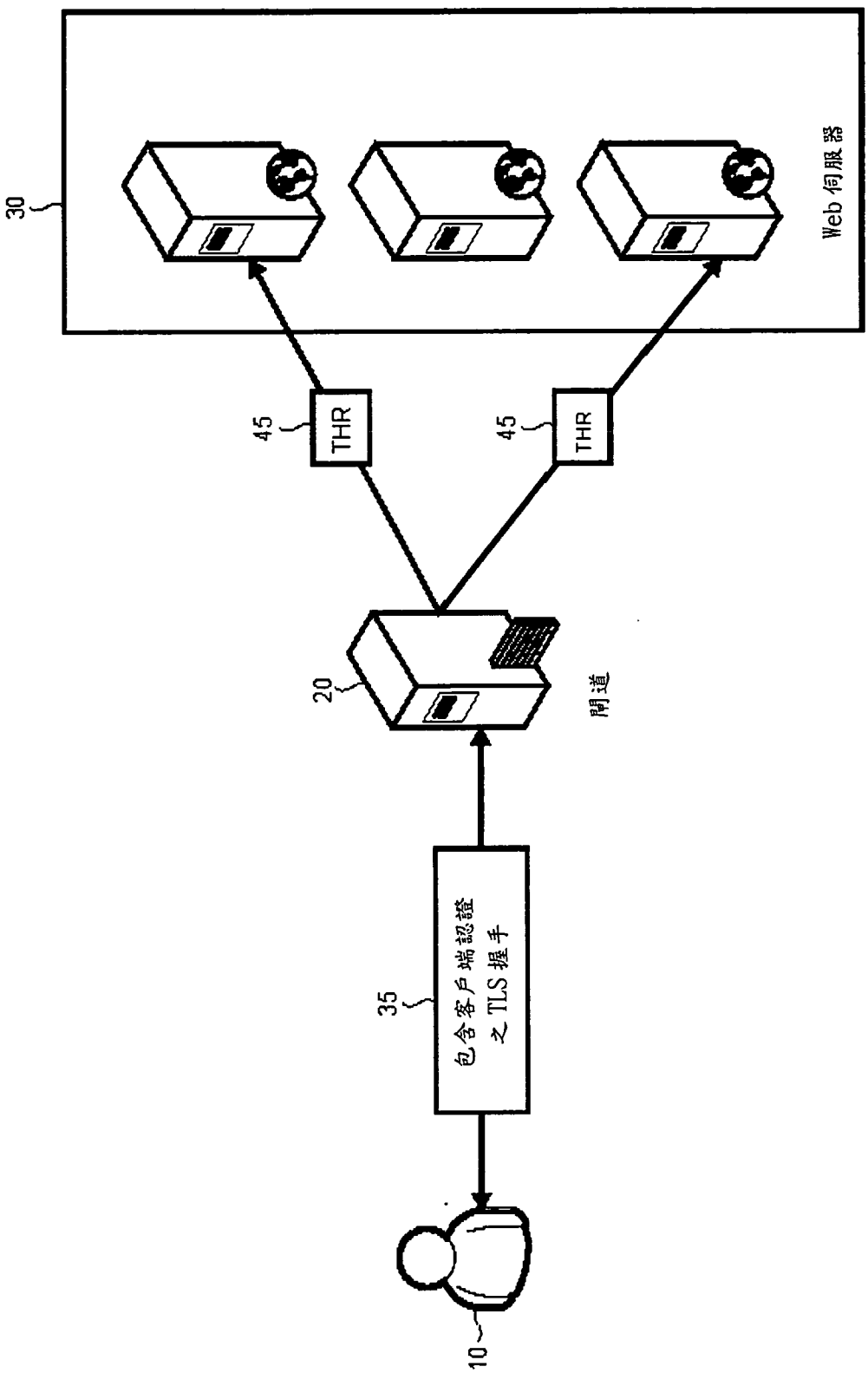
9. 如申請專利範圍第 1 項所述之方法，其中該執行 TLS 握手之步驟更包括以下步驟：

執行第一次握手之步驟，執行一不具客戶端認證的第一次握手；以及

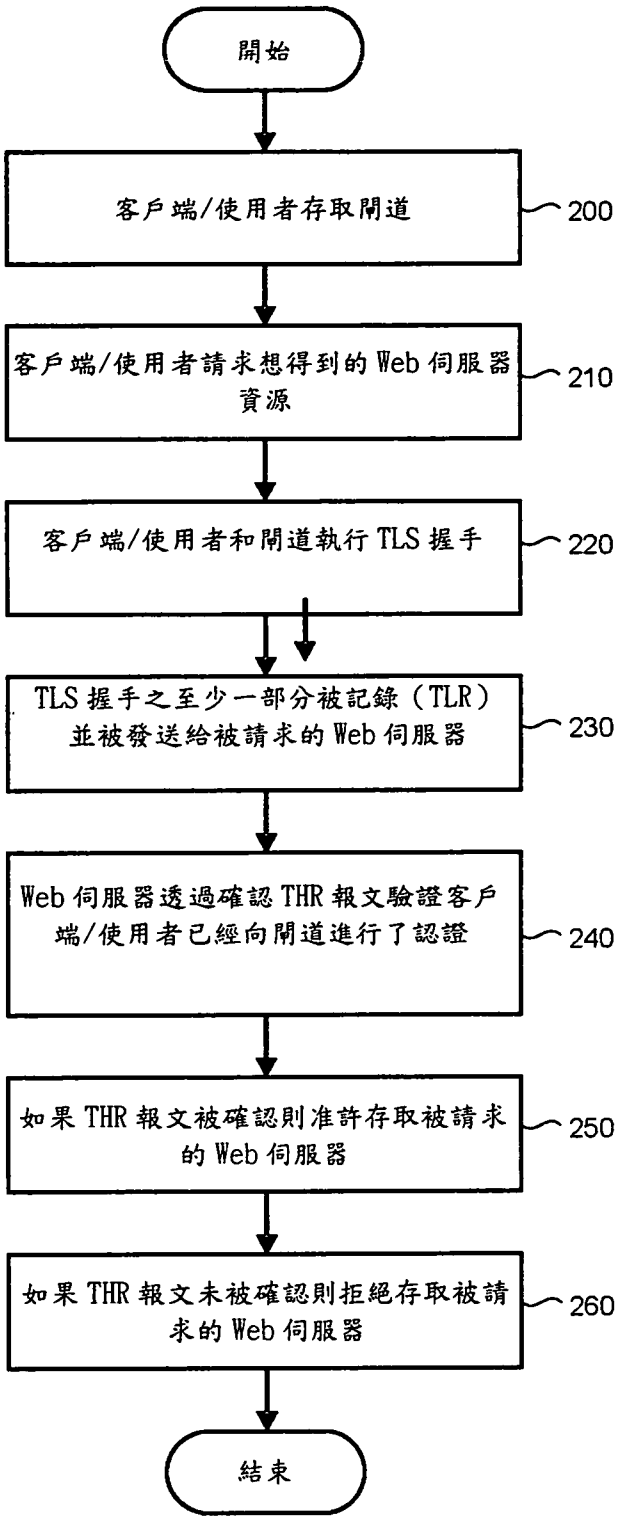
執行第二次握手之步驟，一經成功完成該執行第一次握手之步驟，即執行一具有客戶端認證的第二次握手。

10. 如申請專利範圍第 9 項所述之方法，其中藉由從該第一次握手中得到之一交談金鑰(session key)，來加密該客戶端/使用者與該閘道之間的該第二次握手。

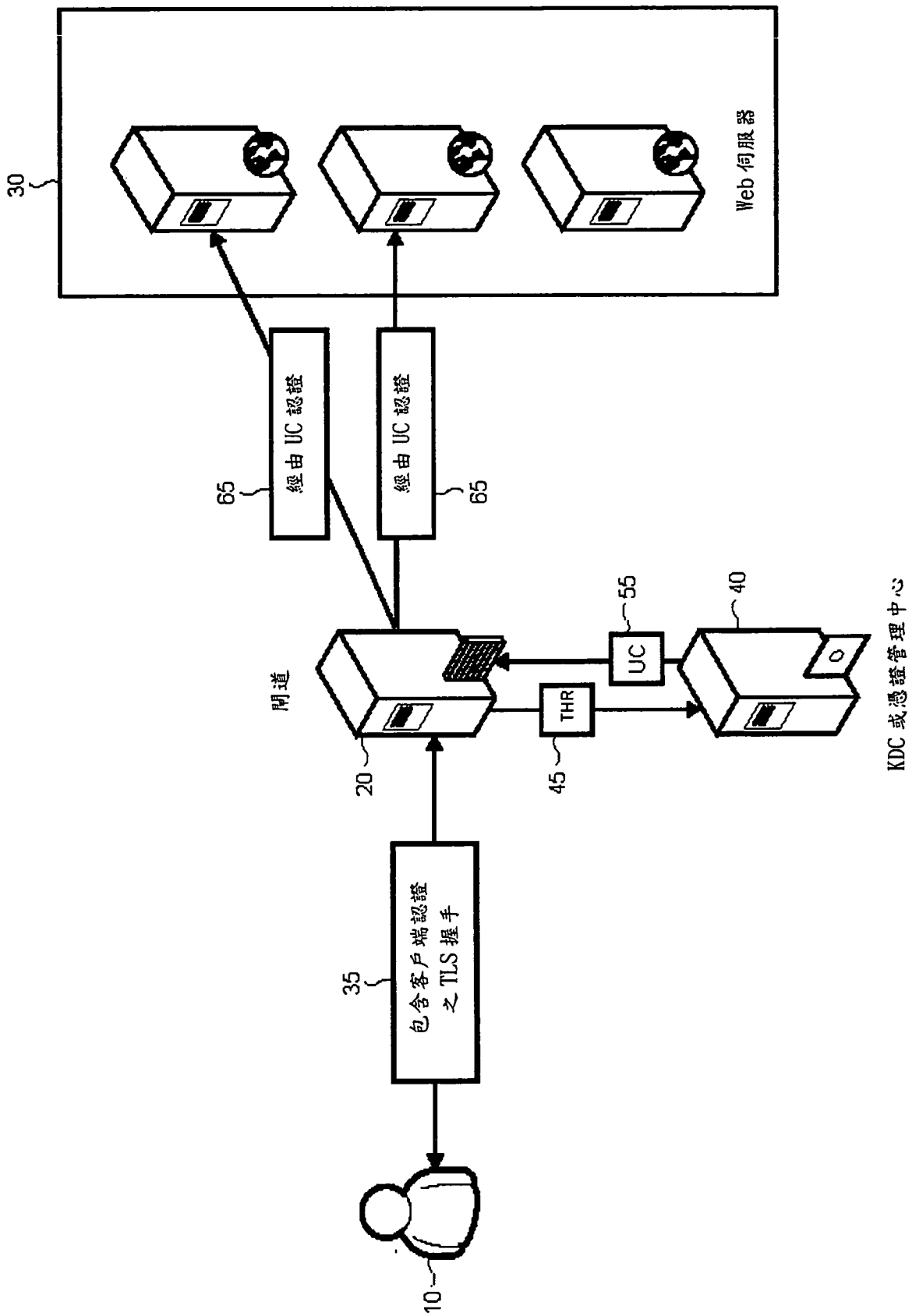
11. 如申請專利範圍第 10 項所述之方法，其中該提供給該服務提供者之記錄係未經加密。



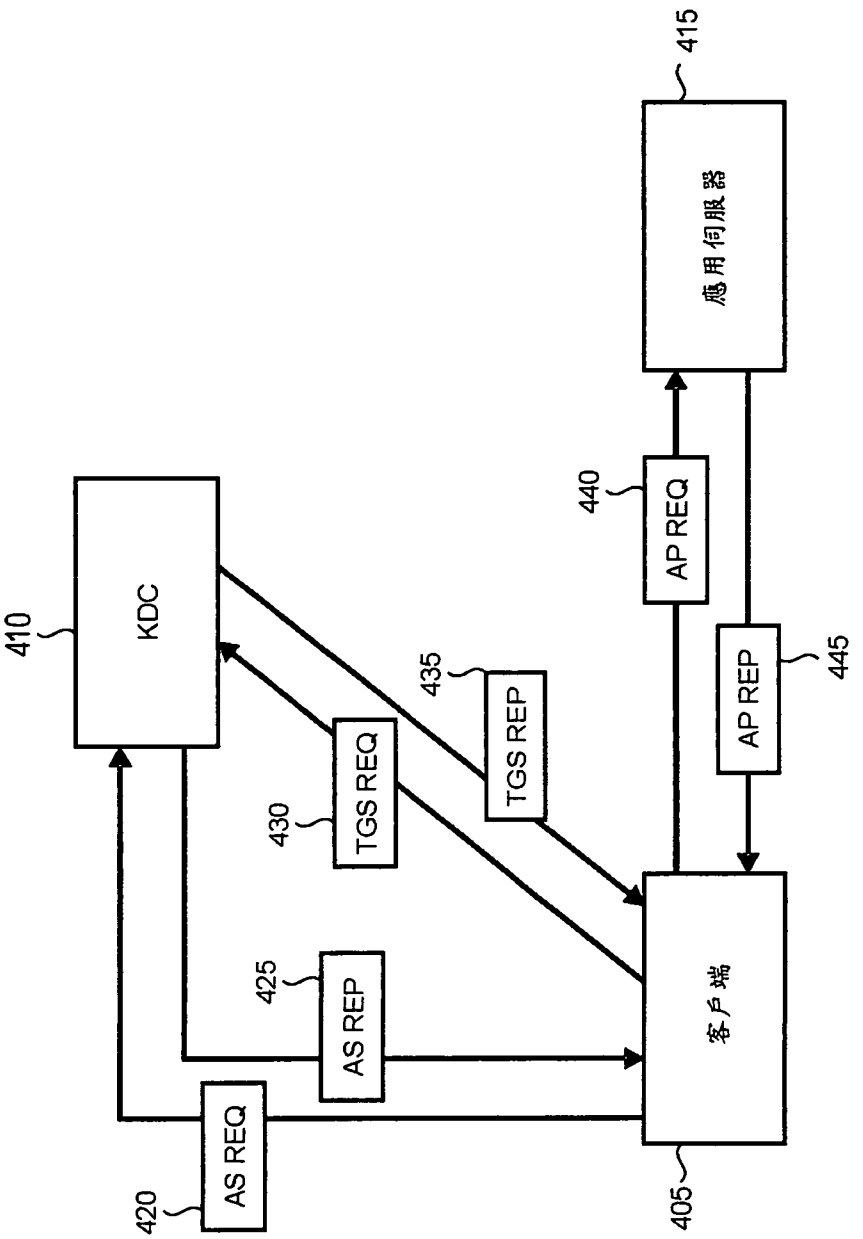
第 1 圖


開始
客戶端/使用者存取閘道
200
客戶端/使用者請求想得到的Web伺服器資源
210
客戶端/使用者和閘道執行TLS握手
220
TLS握手之至少一部分被記錄（TLR）並被發送給被請求的Web伺服器
230
Web伺服器透過確認THR報文驗證客戶端/使用者已經向閘道進行了認證
240
如果THR報文被確認則准許存取被請求的Web伺服器
250
如果THR報文未被確認則拒絕存取被請求的Web伺服器
260
結束

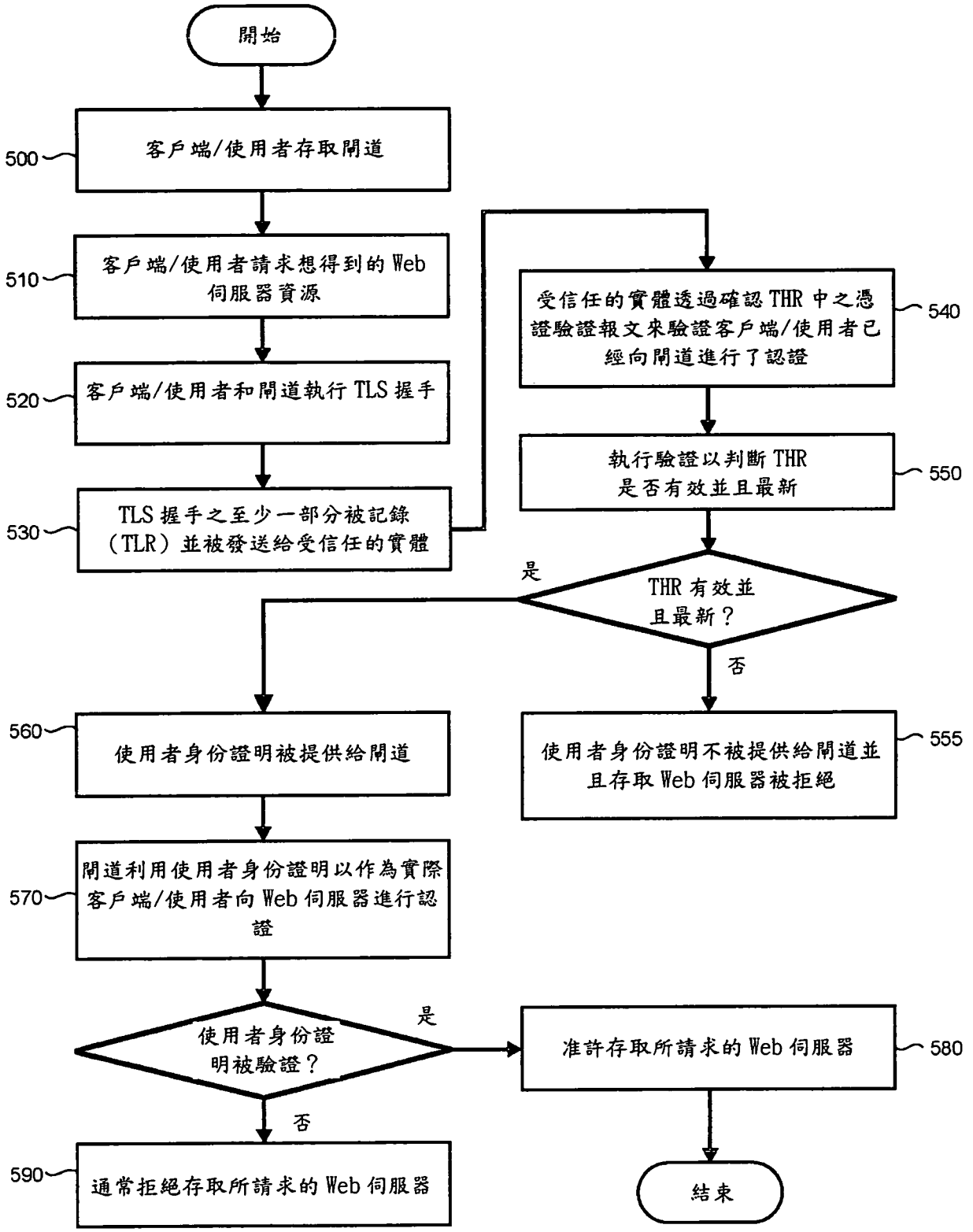
第 2 圖


30
Web 伺服器
經由 UC 認證
65
經由 UC 認證
65
閘道
20
UC
55
THR
45
40
KDC 或憑證管理中心
包含客戶端認證
之 TLS 握手
35
10

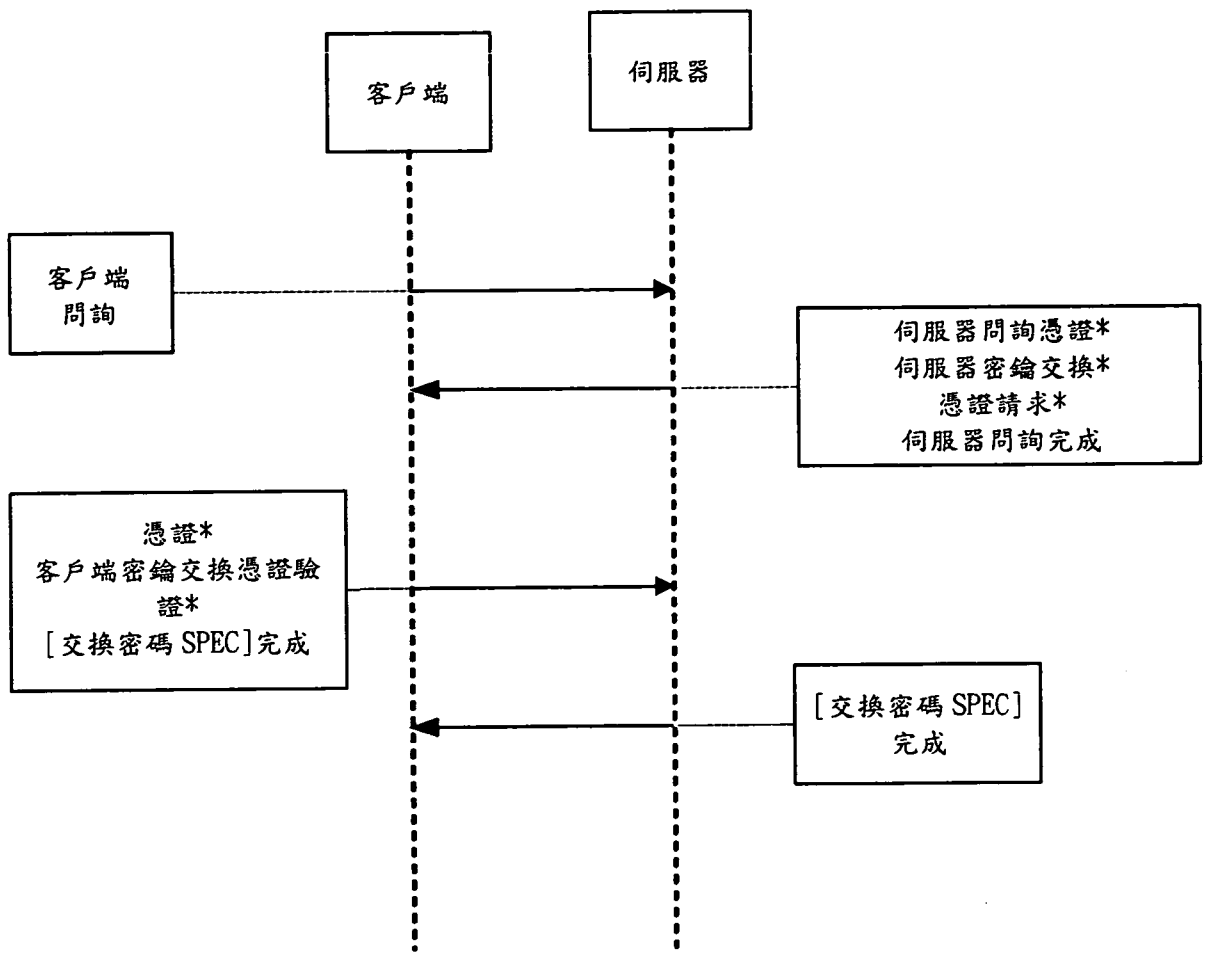
第 3 圖


415
應用伺服器
440
AP REQ
410
KDC
435
TGS REP
445
AP REP
430
TGS REQ
425
AS REP
客戶端
420
AS REQ
405

第 4 圖


開始
500
客戶端/使用者存取閘道
510
客戶端/使用者請求想得到的 Web 伺服器資源
520
客戶端/使用者和閘道執行 TLS 握手
530
TLS 握手之至少一部分被記錄（TLR）並被發送給受信任的實體
540
受信任的實體透過確認 THR 中之憑證驗證報文來驗證客戶端/使用者已經向閘道進行了認證
550
執行驗證以判斷 THR 是否有效並且最新
是
THR 有效並且最新？
否
555
使用者身份證明不被提供給閘道並且存取 Web 伺服器被拒絕
560
使用者身份證明被提供給閘道
570
閘道利用使用者身份證明以作為實際客戶端/使用者向 Web 伺服器進行認證
是
使用者身份證明被驗證？
580
准許存取所請求的 Web 伺服器
否
590
通常拒絕存取所請求的 Web 伺服器
結束

第 5 圖


客戶端
伺服器
客戶端
問詢
伺服器問詢憑證*
伺服器密鑰交換*
憑證請求*
伺服器問詢完成
憑證*
客戶端密鑰交換憑證驗證*
[交換密碼 SPEC]完成
[交換密碼 SPEC]
完成

第 6 圖