(19)中華民國智慧財產局
(12)發明說明書公開本 (11)公開編號：TW 201042973 A1
(43)公開日： 中華民國 99 (2010) 年 12 月 01 日

(21)申請案號：098133284 (22)申請日： 中華民國 98 (2009) 年 09 月 30 日
(51)Int. Cl.： *H04L9/32 (2006.01)*
(30)優先權：2008/11/28 歐洲專利局 08170167.4
(71)申請人：萬國商業機器公司 (美國) INTERNATIONAL BUSINESS MACHINES CORPORATION (US)
美國
(72)發明人：凱斯 艾瑞克 KASS, ERIC (US)
(74)代理人：蔡玉玲
申請實體審查：無 申請專利範圍項數：18 項 圖式數：4 共 32 頁

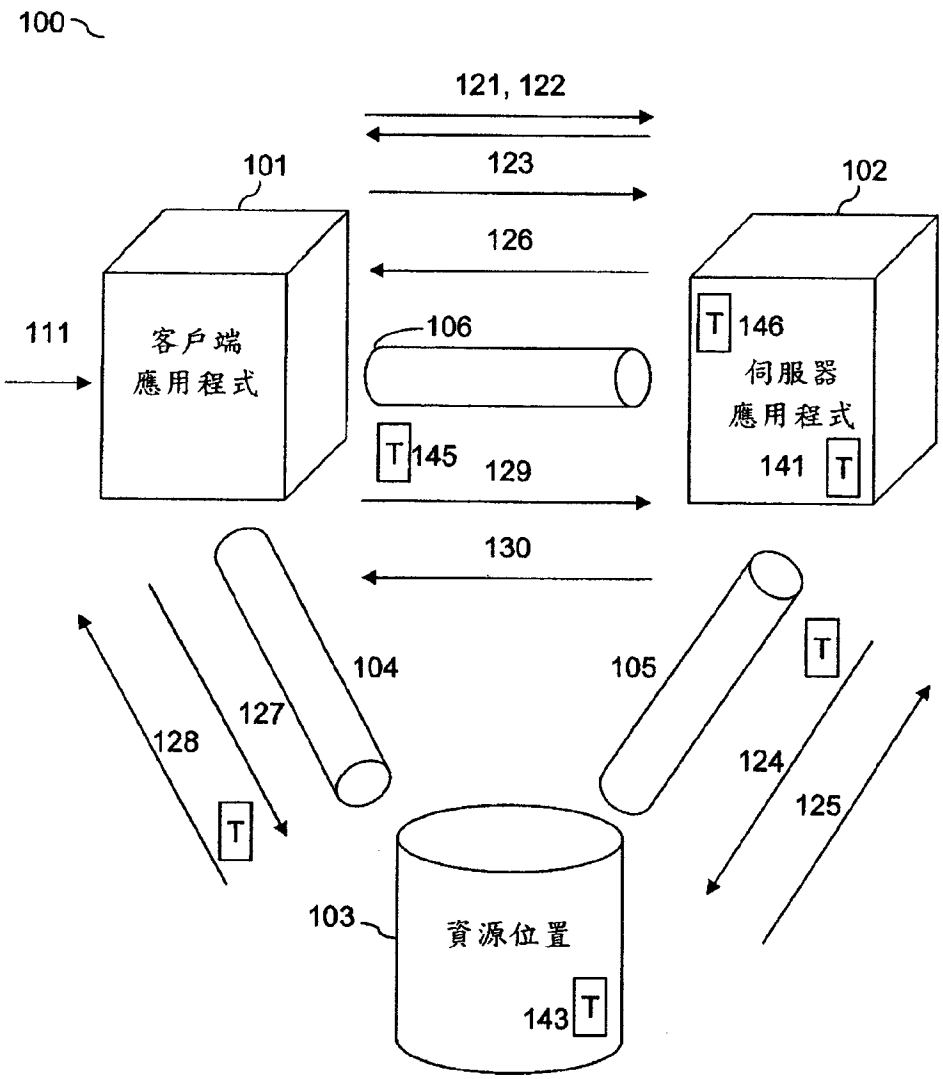
(54)名稱

經由主驗證通訊通道之次通訊通道中基於訊標的客戶端對伺服器之驗證

TOKEN-BASED CLIENT TO SERVER AUTHENTICATION OF A SECONDARY COMMUNICATION CHANNEL BY WAY OF PRIMARY AUTHENTICATED COMMUNICATION CHANNELS

(57)摘要

本發明有關在客戶端應用程式及資源應用程式之間建立已驗證的主通訊通道後，驗證在客戶端應用程式及伺服器應用程式之間的次通訊通道，伺服器應用程式可在資源應用程式上儲存已產生的驗證訊標（token），其只有授權使用者，包括客戶端應用程式使用者，才可以讀取-存取該已產生的驗證訊標及經由次通訊通道將其送回伺服器應用程式。



100：系統
101：客戶端應用程式
102：伺服器應用程式
103：資源位置
104：主通訊通道
105：主通訊通道
106：次通訊通道
141：驗證訊標
143：驗證訊標
145：驗證訊標副本
146：驗證訊標副本

(19)中華民國智慧財產局
(12)發明說明書公開本 (11)公開編號：TW 201042973 A1
(43)公開日： 中華民國 99 (2010) 年 12 月 01 日

(21)申請案號：098133284 (22)申請日： 中華民國 98 (2009) 年 09 月 30 日
(51)Int. Cl.： *H04L9/32 (2006.01)*
(30)優先權：2008/11/28 歐洲專利局 08170167.4
(71)申請人：萬國商業機器公司 (美國) INTERNATIONAL BUSINESS MACHINES CORPORATION (US)
美國
(72)發明人：凱斯 艾瑞克 KASS, ERIC (US)
(74)代理人：蔡玉玲
申請實體審查：無 申請專利範圍項數：18 項 圖式數：4 共 32 頁

(54)名稱

經由主驗證通訊通道之次通訊通道中基於訊標的客戶端對伺服器之驗證

TOKEN-BASED CLIENT TO SERVER AUTHENTICATION OF A SECONDARY COMMUNICATION CHANNEL BY WAY OF PRIMARY AUTHENTICATED COMMUNICATION CHANNELS

(57)摘要

本發明有關在客戶端應用程式及資源應用程式之間建立已驗證的主通訊通道後，驗證在客戶端應用程式及伺服器應用程式之間的次通訊通道，伺服器應用程式可在資源應用程式上儲存已產生的驗證訊標（token），其只有授權使用者，包括客戶端應用程式使用者，才可以讀取-存取該已產生的驗證訊標及經由次通訊通道將其送回伺服器應用程式。

六、發明說明：

【發明所屬之技術領域】

本發明有關在電腦系統中進行驗證的方法、執行該方法的電腦系統、及含有執行該方法之程式碼部分的電腦程式產品。

【先前技術】

客戶端應用程式需要存取伺服器應用程式的資源。客戶端應用程式開啟與伺服器應用程式的通訊通道。此通訊通道通常未經驗證，也就是說任何客戶端應用程式皆可建立連線。在客戶端應用程式存取伺服器應用程式的資源之前，客戶端應用程式請求伺服器應用程式藉由識別客戶端應用程式使用者的名稱進行驗證。為了驗證客戶端應用程式使用者，伺服器應用程式對客戶端應用程式發送詰問，即一種只有真正的客戶端應用程式使用者才能解決的難題。客戶端應用程式送回難題的解答。伺服器應用程式核對解答正確與否，以此方式驗證客戶端應用程式，然後授予伺服器應用程式資源的存取權限給客戶端應用程式。

在先前技術的實施方案中，詰問（challenge）可以是來自伺服器應用程式的訊息，客戶端應用程式以客戶端應用程式使用者的金鑰加密此訊息。此訊息可以是臨時亂數，其已知為安全工程中「使用一次的數字」(“number used once”)，且僅針對一個通訊對話產生。臨時亂數可以是任何隨機資料或時戳（timestamp）。客戶端應用程式使用者的金鑰係客戶端應用程式及伺服器應用程式二者均有副本的對稱金鑰。或者，金鑰係非對稱金鑰，其中客戶端應用程式具有私密金鑰，及伺服器應用

程式具有對應的公開金鑰。客戶端將加密訊息送回伺服器應用程式。伺服器應用程式分別用客戶端應用程式使用者的對稱金鑰或公開金鑰解密此訊息，然後核對此解密訊息是否匹配伺服器應用程式已發送給客戶端應用程式的訊息。當核對成功後，伺服器應用程式推斷此訊息已由客戶端應用程式使用者之各別對稱金鑰或私密金鑰的持有者加密，然後驗證加密訊息的發送者。

在先前技術中，另一種驗證方式係基於用非對稱金鑰對密碼的加密及解密。客戶端應用程式經由加密通訊通道，發送密碼給伺服器應用程式。通訊通道可用伺服器應用程式使用者的公開金鑰加密，該公開金鑰不是可公開取得，就是在加密密碼且經由通訊通道將其發送給伺服器應用程式之前，已經傳遞給客戶端應用程式。只有伺服器應用程式才能用伺服器應用程式使用者的私密金鑰解密含有密碼的接收訊息。當伺服器應用程式運行於伺服器應用程式主機上時，伺服器應用程式可使用得自客戶端應用程式的密碼，請求伺服器應用程式主機的基本作業系統進行驗證。

在先前技術中，Kerberos 演算法使用伺服器應用程式經由中央驗證伺服器對客戶端應用程式的驗證。詳情請見例如 C. Kaufman 等人的「網路安全(Network Security)」，Prentice Hall 出版社，2002 年。Kerberos 演算法實質上運作如下：客戶端應用程式發送請求至中央驗證伺服器，要求傳回由伺服器應用程式用於驗證的票證。驗證伺服器藉由伺服器應用程式使用者的公開或對稱金鑰加密對話金鑰及客戶端應用程式使用者的名

稱，為伺服器應用程式設計對話金鑰及產生票證。為伺服器應用程式設計的對話金鑰、產生的票證、及伺服器應用程式使用者的名稱全部都用客戶端應用程式使用者的公開或對稱金鑰來加密。中央驗證伺服器將加密訊息發送給客戶端應用程式。只有客戶端應用程式使用者才能夠用客戶端應用程式使用者的私密或對稱金鑰解密接收的訊息。客戶端應用程式使用者核對接收自中央驗證伺服器的訊息是否可用來由伺服器應用程式驗證客戶端應用程式，因為只有客戶端應用程式使用者能夠解密訊息且該訊息含有伺服器應用程式使用者的名稱。客戶端應用程式將伺服器應用程式的票證及用對話金鑰加密的時戳發送給伺服器應用程式。只有伺服器應用程式使用者才能夠用伺服器應用程式使用者的私密或對稱金鑰解密票證並擷取對話金鑰及客戶端應用程式使用者的名稱。伺服器應用程式認可中央驗證伺服器已插入票證中的客戶端應用程式使用者名稱，因而此票證可用來由伺服器應用程式驗證發送的客戶端應用程式。伺服器應用程式使用來自解密票證的對話金鑰解密加密的時戳並加以確認。根據票證及時戳，伺服器應用程式授予存取權限給請求存取伺服器應用程式的客戶端應用程式。

中央驗證伺服器的加密保證只有客戶端應用程式使用者才能解密來自中央驗證伺服器的訊息，而且只有伺服器應用程式使用者才能解密中央驗證伺服器所產生及客戶端應用程式已發送至伺服器應用程式的票證。

在 Kerberos 演算法中，客戶端應用程式使用者自行與伺服器應用程式進行驗證，不用知道伺服器應用程式使用者的密碼

或金鑰。反之亦然，伺服器應用程式也不需要儲存客戶端應用程式使用者的任何金鑰或密碼。然而，中央驗證伺服器必須儲存客戶端應用程式使用者及伺服器應用程式使用者二者的公開或對稱金鑰。

先前技術在伺服器應用程式無法存取基本作業系統的驗證機制時具有缺點。在此情況下，伺服器應用程式無法使用接收自客戶端應用程式的密碼驗證客戶端應用程式使用者。

先前技術的第二個缺點是傳送任何密碼時均必須加密通訊通道的事實。客戶端應用程式及伺服器應用程式中至少一個必須對經由通訊通道安全交換資料所需的密碼或臨時亂數進行加密及解密。加密及解密程式碼的實施方案很複雜。

Kerberos 演算法係基於具票證產生機制的中央驗證伺服器及使用客戶端應用程式使用者及伺服器應用程式使用者的對稱或非對稱金鑰對訊息的加密及解密。驗證伺服器的設定及實施方案及在客戶端應用程式側及伺服器應用程式側用於加密及解密的程式碼也是很複雜。

【發明內容】

因此本發明之目的係提供一種用於驗證的簡化方法及系統：在客戶端應用程式及伺服器應用程式之間建立未驗證及未加密次通訊通道之後，由伺服器應用程式驗證客戶端應用程式。

本發明此目的可以在具有以下項目之系統中的驗證方法來

達成：客戶端應用程式、伺服器應用程式、資源位置、在客戶端應用程式及資源位置之間的驗證主通訊通道、及在伺服器應用程式及資源位置之間的驗證主通訊通道。驗證通訊通道是指由資源位置驗證在客戶端應用程式及資源位置之間建立通訊通道的客戶端應用程式使用者。相同的道理也適用於在伺服器應用程式及資源位置之間的驗證通訊通道，其中資源位置驗證伺服器應用程式使用者。資源位置僅允許一組授權使用者建立通訊通道，且知道與資源位置建立通訊通道的使用者身分。主通訊通道不一定要加密，也就是說入侵的應用程式可在通訊通道上竊聽並讀取傳送的訊息。

為了建立在客戶端應用程式及伺服器應用程式之間的直接次通訊通道連線，客戶端應用程式建立與伺服器應用程式的次通訊通道，其通常為未驗證及未加密。任何客戶端應用程式皆可與伺服器應用程式建立通訊通道。伺服器應用程式並不知道建立通訊通道連線的客戶端應用程式使用者身分。客戶端應用程式經由次通訊通道對伺服器應用程式提出授予存取權限的請求，並告知伺服器應用程式客戶端應用程式使用者的身分。伺服器應用程式按以下方式驗證客戶端應用程式使用者：伺服器應用程式啟始驗證訊標的產生。伺服器應用程式可自行產生驗證訊標或請求遠端伺服器產生驗證訊標。驗證訊標可以是使用一次的某個臨時亂數、數字或字組，例如，在統計上為隨機的位元型樣或加密時戳(timestamp)。伺服器應用程式啟始以儲存驗證訊標於資源位置處，並設定存取權限讓客戶端應用程式使用者具有存取驗證訊標的權利。在伺服器應用程式儲存產生的驗證訊標於資源位置處後，伺服器應用程式使用者具有存取資

源位置的寫入及產生權限、儲存驗證訊標於資源位置處、及設定存取權限，因此僅授權使用者，包括客戶端應用程式使用者，獲准經由在客戶端應用程式及資源位置之間的驗證主通訊通道存取驗證訊標。客戶端應用程式必須至少具有讀取驗證訊標的權限。請求存取伺服器應用程式的非授權使用者不得有存取驗證訊標的權利，因而也沒有讀取或修改驗證訊標的權利。伺服器應用程式使用者及可能系統管理員通常屬於授權使用者，因而具有存取驗證訊標的權限。客戶端應用程式經由在客戶端應用程式及資源位置之間的驗證主通訊通道擷取驗證訊標副本。客戶端應用程式經由次通訊通道將驗證訊標副本傳回伺服器應用程式。在伺服器應用程式啟始後，伺服器應用程式隨即檢查客戶端應用程式傳回的驗證訊標副本是否匹配儲存於資源位置處之產生的驗證訊標。在伺服器應用程式證實所接收的驗證訊標副本及所儲存的驗證訊標完全相同後，伺服器應用程式驗證客戶端應用程式、經由次通訊通道將成功訊息傳回客戶端應用程式、及授予存取權限給客戶端應用程式。當所接收的驗證訊標副本與所儲存的驗證訊標不同時，伺服器應用程式經由次通訊通道傳回錯誤訊息，並拒絕客戶端應用程式的存取。

在本發明之一較佳具體實施例中，在產生的驗證訊標儲存於資源位置處之前，客戶端應用程式已與伺服器應用程式建立次通訊通道。次通訊通道是伺服器應用程式預期從客戶端應用程式接收驗證訊標所利用的唯一通訊通道。這表示主通訊通道未必要加密。當入侵的客戶端應用程式在任何主驗證通訊通道上竊聽、讀取驗證訊標、及建立與伺服器應用程式的另一次通訊通道時，伺服器應用程式將拒絕入侵客戶端應用程式的存

取，因為與請求之客戶端應用程式的次通訊通道已經建立。

客戶端應用程式在客戶端裝置中運行，及伺服器應用程式在伺服器裝置中運行。資源位置位在客戶端裝置、伺服器裝置、及第三裝置其中之一。

在本發明的較佳具體實施例中，客戶端裝置及伺服器裝置屬於各具有獨立檔案系統的獨立主機系統，及資源位置是伺服器應用程式主機的本機檔案系統。客戶端應用程式主機將伺服器應用程式主機的檔案系統掛載為遠端檔案系統，並使用作業系統服務提供的遠端檔案系統之掛載的驗證機制存取遠端檔案系統的檔案。伺服器應用程式使用本機檔案系統的作業系統服務，其基本上會驗證伺服器應用程式使用者，以授予本機檔案系統之檔案的存取權限。

在本發明的較佳具體實施例中，客戶端應用程式是資料庫驅動程式的客戶端元件，及伺服器應用程式是資料庫驅動程式的伺服器元件。

在本發明之一替代性具體實施例中，客戶端應用程式及伺服器應用程式係在相同的裝置中運行。這表示二者均可執行於具有一個本機檔案系統的相同主機系統中。客戶端應用程式發送要求授予存取權限的請求給伺服器應用程式。請求包括客戶端應用程式使用者的名稱，但不包括密碼。伺服器應用程式無法使用客戶端應用程式使用者的密碼，因為伺服器應用程式無法存取基本作業系統的驗證機制。伺服器應用程式儲存產生的

驗證訊標於共同檔案系統的位置處，客戶端應用程式在該處可輕易地讀取驗證訊標。客戶端應用程式將驗證訊標副本發送給伺服器應用程式。伺服器應用程式核對驗證訊標後，授予存取權限給客戶端應用程式。

在本發明之一第二替代性具體實施例中，資源位置係檔案伺服器主機的檔案系統，檔案伺服器主機係與客戶端應用程式主機及伺服器應用程式主機分開。客戶端應用程式主機及伺服器應用程式主機分別將檔案伺服器主機的檔案系統掛載為遠端檔案系統，並使用作業系統服務提供的驗證機制存取遠端檔案系統的檔案。

在本發明之一第三替代性具體實施例中，資源位置可以是驗證伺服器或資料庫伺服器。

在本發明之一第四替代性具體實施例中，在客戶端應用程式及資源位置之間的主通訊通道及在伺服器應用程式及資源位置之間的主通訊通道中至少一個使用驗證的網路通訊協定。網路通訊協定可以是安全通訊端層(SSL)，及儲存於資源位置處的驗證訊標可由統一資源定位器(URL)識別。

在本發明之一第五替代性具體實施例中，在客戶端應用程式建立與伺服器應用程式的次通訊通道之前，伺服器應用程式啟始以將產生的驗證訊標儲存於資源位置處。客戶端應用程式使用者可存取及讀取驗證訊標、建立與伺服器應用程式的次通訊通道、發送驗證訊標副本給伺服器應用程式，最後由伺服器

應用程式驗證客戶端應用程式。然而，在此情況下，主通訊通道必須加密。當主通訊通道未加密時，入侵的客戶端應用程式可在任何主通訊通道上竊聽、建立與伺服器應用程式的次通訊通道、佯裝是驗證訊標為其所產生的客戶端應用程式使用者、濫用所竊取的驗證訊標副本並將其發送給伺服器應用程式、及取得授予伺服器應用程式的存取權限。

在本發明之第六替代性具體實施例中，以伺服器應用程式替換客戶端應用程式，反之亦然。以在伺服器應用程式及資源位置之間的主通訊通道替換在客戶端應用程式及資源位置之間的主通訊通道，反之亦然。在客戶端應用程式及伺服器應用程式之間的如此角色交換之後，可按對應的方式應用所說明的驗證方法。

在本發明之第七替代性具體實施例中，客戶端應用程式及伺服器應用程式中至少一個在智慧卡裝置中運行。

本發明方法可施行於電腦系統中，並可實施於電腦程式產品中，以在包含施行本方法步驟之電腦程式碼部分的資料處理系統中執行。

【實施方式】

在圖式及說明書中提出本發明的較佳具體實施例，雖然使用特定用語，但如此提供的說明僅針對一般及描述的意義使用，而非用來限制。然而，應明白，只要不脫離如隨附申請專利範圍所述之本發明的廣泛精神及範疇，可對本發明進行修改

及變更。

本發明可以硬體、軟體、或硬體及軟體的組合來實現。任何種類的電腦系統或其他適於執行本文所述方法的設備都很合適。典型的硬體與軟體組合可以是具有載入及執行時可控制電腦系統以執行本文所述方法之電腦程式的通用電腦系統。本發明亦可內建在電腦程式產品中，電腦程式產品包含實施本文所述方法的所有特色，且電腦程式產品在被載入電腦系統中後，還可以執行這些方法。

本文中的電腦程式構件或電腦程式係指任何用來使具有資訊處理能力的系統能夠直接或在以下項目之一或二者之後：a)轉換成另一種語言、程式碼或標記；b)以不同的材料形式再現，施行特定功能之一組指令之任何語言、程式碼或標記的表示。

圖 1 顯示一種用於驗證的系統，其包含：客戶端應用程式(101)、伺服器應用程式(102)、及資源位置(103)。客戶端應用程式(101)及伺服器應用程式(102)分別經由已驗證的主通訊通道(104)及(105)存取資源位置(103)。

主通訊通道(104)及(105)未必要加密，也就是說，第三方可以讀取在通道(104)及(105)上傳送的資料。通訊通道(104)提供路徑讓客戶端應用程式能夠存取資源位置(103)之控制存取權限的資源，例如，遠端檔案系統中控制存取權限的檔案。

客戶端應用程式(101)代表客戶端應用程式使用者在驗證登

入對話中運行，客戶端應用程式使用者藉由輸入使用者名稱及密碼，登入(111)客戶端應用程式。

伺服器應用程式(102)代表伺服器應用程式使用者，在由作業系統服務建立的驗證登入對話(logon session)中運行。

客戶端應用程式(101)預計建立與伺服器應用程式(102)的次通訊通道(106)。次通訊通道(106)可以是在資料庫驅動程式之客戶端及伺服器元件之間連接客戶端應用程式與資料庫伺服器的通訊端。資料庫驅動程式的伺服器元件可能無法存取資料庫伺服器之基本作業系統的驗證機制並使用客戶端應用程式使用者的接收密碼進行驗證。因此，客戶端應用程式(101)建立(121、122)與伺服器應用程式(102)之次要的未驗證次通訊通道(106)，這表示通訊通道不需要使用者憑證，任何客戶端應用程式均可建立此連線。通訊通道(106)未必要加密。

客戶端應用程式(101)透過所建立之未驗證的次通訊通道(106)，發送請求(123)給伺服器應用程式(102)，要求驗證代表客戶端應用程式使用者運行的客戶端應用程式。此請求含有客戶端應用程式使用者的名稱。

伺服器應用程式(102)產生驗證訊標(141)，其可以是在統計上為隨機的位元型樣或加密時戳。身分確認的可信度由驗證訊標(141)的隨機產生器品質決定。伺服器應用程式「放下(drop it off)」(124、125)驗證訊標(143)於資源位置(103)處，也就是說，以特定的名稱及位置加以儲存。伺服器應用程式設定驗證訊標

(143)的檔案存取權限，因而僅有一組授權使用者，包括客戶端應用程式使用者，獲准讀取驗證訊標。客戶端應用程式使用者的名稱包含在請求(123)中，以驗證與伺服器應用程式的次通訊通道。然而，非授權使用者不得存取驗證訊標。伺服器應用程式使用者及通常是系統管理員，屬於具有存取驗證訊標(143)之權利的一組授權使用者。

伺服器應用程式(102)經由次通訊通道(106)，將回應傳回(126)客戶端應用程式(101)，回應包括儲存於資源位置(103)處之驗證訊標(143)的名稱及位置。

客戶端應用程式(101)經由驗證主通訊通道(104)「恢復(recover)」，也就是說，讀取(127、128)，資源位置(103)的驗證訊標。請求與具有客戶端應用程式使用者憑證之伺服器應用程式(102)或任何應用程式使用者之次通訊通道(106)的客戶端應用程式使用者是獲准存取及讀取驗證訊標(143)的授權使用者之一。客戶端應用程式(101)經由次通訊通道(106)，將驗證訊標(143)的副本(145)傳回(129)伺服器應用程式(102)。

伺服器應用程式(102)透過預期的次通訊通道(106)接收驗證訊標(143)的副本(146)。這是伺服器應用程式(102)為了回應驗證客戶端應用程式使用者的請求(123)，預期可在其上接收驗證訊標(143)之副本(146)的唯一通訊通道。

伺服器應用程式核對(102)所接收(所恢復)之驗證訊標(143)的副本(146)是否匹配伺服器應用程式已儲存(「放下」)於資源

位置(103)且只有客戶端應用程式使用者才能存取的驗證訊標(143)。儲存的驗證訊標(143)與產生的驗證訊標(141)完全相同。

如果核對成功，則建立與伺服器應用程式(102)之未驗證次通訊通道(106)的使用者係其所宣稱的使用者。伺服器應用程式(102)驗證與客戶端應用程式的次通訊通道(106)並授予存取權限給客戶端應用程式(101)。伺服器應用程式可經由次通訊通道(106)，將客戶端應用程式使用者已經驗證的確認訊息傳回(130)客戶端應用程式。

如果核對失敗，也就是說，如果驗證訊標的副本(146)不同於所儲存的驗證訊標(143)或不同於所產生的驗證訊標(141)，則伺服器應用程式拒絕存取並經由次通訊通道(106)，將應用程式錯誤傳回(130)客戶端應用程式。

如果在客戶端應用程式(101)及資源位置(103)之間的主通訊通道(104)及在伺服器應用程式(102)及資源位置(103)之間的主通訊通道中至少一個未加密，則重要的是，在伺服器應用程式儲存驗證訊標於資源位置(103)處“之前”，建立與伺服器應用程式(102)之未驗證的次通訊通道(106)。伺服器應用程式(102)預期僅利用所建立之次通訊通道(106)的驗證訊標。

圖 2 含有本發明驗證方法的流程圖及程序圖。為回應建立次通訊通道(106)的請求(211)，客戶端應用程式(201)建立(212、231、232)與伺服器應用程式(202)的未驗證次通訊通道(106)。客戶端應用程式(201)使用此通訊通道(106)提出請求(213、233)至

伺服器應用程式(202)。伺服器應用程式(202)產生(214)驗證訊標並將其儲存(215、234、235)於資源位置(203)，讓客戶端應用程式使用者是除了伺服器應用程式使用者及可能系統管理員之外，唯一能夠讀取驗證訊標的使用者。伺服器應用程式(202)將回應傳回(216、236)客戶端應用程式(201)。接著，客戶端應用程式(201)經由在客戶端應用程式(201)及資源位置(203)之間的主通訊通道(104)，擷取(217、237、238)驗證訊標副本，並使用次通訊通道(106)將其傳回(218、239)伺服器應用程式(202)。伺服器應用程式(202)核對(219)所接收的驗證訊標副本是否匹配儲存於資源位置(203)及只有客戶端應用程式使用者才能讀取-存取之所產生的驗證訊標。如果核對成功，則伺服器應用程式經由次通訊通道(106)傳回(220、240)成功訊息及授予存取權限(222)給客戶端應用程式(201)。如果核對失敗，則伺服器應用程式(202)利用次通訊通道(106)，將錯誤訊息送回(221、240)客戶端應用程式(201)，並拒絕(223)客戶端應用程式(201)的存取。

圖 3 顯示一替代性具體實施例，其中在客戶端應用程式(301)及伺服器應用程式(302)之間的次通訊通道(106)已經建立之前，伺服器應用程式(302)在啟始化(311)後即產生(312)驗證訊標，並將其儲存(313、321、322)於資源位置(303)。在替代性具體實施例中，在所產生的驗證訊標及預期建立與伺服器應用程式之次通訊通道(106)並將驗證訊標副本發送給伺服器應用程式的客戶端應用程式使用者之間，存在一對一的關係。

圖 4 顯示替代性具體實施例的方法步驟，其中在建立次通訊通道之前，產生的驗證訊標已儲存於資源位置(403)處。為回

應驗證代表客戶端應用程式使用者運行之客戶端應用程式經由次通訊通道(106)的請求(411)，客戶端應用程式自資源位置(403)擷取(412、421、422)驗證訊標副本。除了伺服器應用程式使用者及可能系統管理使用者，只有客戶端應用程式使用者是存取驗證訊標的授權使用者。

客戶端應用程式產生(413、423、424)與伺服器應用程式之未驗證的次通訊通道(106)，並經由次通訊通道(106)將驗證訊標副本傳回(414、425)伺服器應用程式。伺服器應用程式核對(415)接收的驗證訊標副本是否匹配伺服器應用程式已針對特定的客戶端應用程式使用者儲存的驗證訊標。根據核對的結果，伺服器應用程式發送(426)成功訊息(416)或錯誤訊息(417)，並分別授予存取權限(418)給客戶端應用程式或拒絕(419)客戶端應用程式的存取。

如果在客戶端應用程式(101)及資源位置(103)之間的主通訊通道(104)及在伺服器應用程式(102)及資源位置(103)之間的主通訊通道(105)中至少一個未加密，則第三方可自通訊通道讀取驗證訊標副本、建立與伺服器應用程式的未驗證次通訊通道，及宣稱是驗證訊標為其產生的客戶端應用程式使用者。為了避免在建立次通訊通道(106)之前儲存驗證訊標於資源位置處的情況中濫用驗證訊標，在客戶端應用程式(101)及資源位置(103)之間的主通訊通道(104)及在伺服器應用程式(102)及資源位置(103)之間的主通訊通道(105)必須加密。

當第一次經由客戶端應用程式(101)及伺服器應用程式(102)

之間的次通訊通道(106)傳送驗證訊標時，伺服器應用程式通常在入侵的客戶端應用程式可以在次通訊通道(106)上竊聽及讀取驗證訊標副本之前接收驗證訊標副本。在此情況下，次通訊通道未必要加密。當任何驗證訊標副本在至少一個通訊通道上傳送至少多次時，即使依序使用多個通訊通道，也必須加密對應的通訊通道。客戶端應用程式(101)可以恰如客戶端應用程式使用者以伺服器應用程式驗證的相同方式，核對伺服器應用程式使用者的身分，只要交換以下角色即可：客戶端應用程式(101)與伺服器應用程式(102)，以及在客戶端應用程式(101)及資源位置(103)之間的主通訊通道(104)與在伺服器應用程式(102)及資源位置(103)之間的主通訊通道(105)。在如此反向驗證的例子中，伺服器應用程式建立與客戶端應用程式的未驗證次通訊通道(106)、提出要求授予存取權限的請求至客戶端應用程式。客戶端應用程式啟始產生驗證訊標並將其儲存於資源位置處，驗證訊標可由請求授予權限存取的伺服器應用程式使用者讀取存取。伺服器應用程式經由驗證主通訊通道(105)擷取資源位置的驗證訊標副本，並經由次通訊通道(106)將驗證訊標副本傳回客戶端應用程式。客戶端應用程式核對由伺服器應用程式傳回的驗證訊標副本是否匹配客戶端應用程式儲存於資源位置(103)的驗證訊標。

【圖式簡單說明】

本發明藉由舉例加以說明且不受圖式中圖解形狀的限制，其中：

圖 1 為根據本發明之基於訊標之驗證系統的方塊圖。

圖 2、3、及 4 為根據本發明之基於驗證訊標之驗證方法的

流程圖及程序圖。

【主要元件符號說明】

100	系統
101、201、301、401	客戶端應用程式
102、202、302、402	伺服器應用程式
103、203、303、403	資源位置
104、105	主通訊通道
106	次通訊通道
141、143	驗證訊標
145、146	驗證訊標副本

201042973

發明專利說明書

（本說明書格式、順序，請勿任意更動，※記號部分請勿填寫）

※ 申請案號：98133284

※ 申請日：98年09月30日　　※IPC 分類：H04L 9/32 (2006.01)

一、發明名稱：（中文/英文）

經由主驗證通訊通道之次通訊通道中基於訊標的客戶端對伺服器之驗證

TOKEN-BASED CLIENT TO SERVER AUTHENTICATION OF A SECONDARY COMMUNICATION CHANNEL BY WAY OF PRIMARY AUTHENTICATED COMMUNICATION CHANNELS

二、中文發明摘要：

本發明有關在客戶端應用程式及資源應用程式之間建立已驗證的主通訊通道後，驗證在客戶端應用程式及伺服器應用程式之間的次通訊通道，伺服器應用程式可在資源應用程式上儲存已產生的驗證訊標（token），其只有授權使用者，包括客戶端應用程式使用者，才可以讀取-存取該已產生的驗證訊標及經由次通訊通道將其送回伺服器應用程式。

三、英文發明摘要：

The disclosure relates to authenticating a secondary communication channel between a client application and a server application when an authenticated primary communication channel has already been established between the client application and a resource application, on which

the server application can store a generated authentication token that only privileged users including the client application user can read-access and send back to the server application by way of the secondary communication channel.

七、申請專利範圍：

1. 一種在一系統中進行驗證的方法，該系統具有：一客戶端應用程式、一伺服器應用程式、一資源位置、一在該客戶端應用程式及該資源位置之間的驗證主通訊通道、及一在該伺服器應用程式及該資源位置之間的驗證主通訊通道，該方法包含以下步驟：

該客戶端應用程式建立一與該伺服器應用程式的次通訊通道；

該客戶端應用程式經由該次通訊通道提出一請求至該伺服器應用程式，要求授予存取權限；

該伺服器應用程式在該驗證成功後，經由該次通訊通道授予存取權限給該客戶端應用程式；

該方法特徵在於其另外包含以下步驟：

該伺服器應用程式啟始將要儲存於該資源位置之一驗證訊標的產生，該客戶端應用程式可經由在該客戶端應用程式及該資源位置之間的該驗證主通訊通道存取該驗證訊標；

該客戶端應用程式經由在該客戶端應用程式及該資源位置之間的該驗證主通訊通道擷取該資源位置的該驗證訊標；

該客戶端應用程式經由該次通訊通道將該驗證訊標傳回該伺服器應用程式；

該伺服器應用程式藉由檢查該客戶端應用程式傳回該伺服器應用程式的該驗證訊標是否匹配該伺服器應用程式啟始後儲存於該資源位置之該產生的驗證訊標，驗證該客戶端應用程式。

2. 如申請專利範圍第 1 項所述之方法，其中該驗證訊標僅可由授權的使用者存取，授權的使用者包括請求存取該伺服器應用程式的該客戶端應用程式。

3. 如申請專利範圍第 1 項所述之方法，其中針對在該客戶端應用程式及該伺服器應用程式之間的該次通訊通道的單一建立，產生儲存於該資源位置的該驗證訊標。

4. 如申請專利範圍第 1 項所述之方法，其中該產生的驗證訊標係一在統計上為隨機的位元型樣(bit pattern)。

5. 如申請專利範圍第 1 項所述之方法，其中該資源位置係一檔案系統。

6. 如申請專利範圍第 5 項所述之方法，其中該檔案系統係該伺服器應用程式及該客戶端應用程式中至少一個的一本機檔案系統。

7. 如申請專利範圍第 5 項所述之方法，其中在該客戶端應用程式及該資源位置之間的該主通訊通道及在該伺服器應用程式及該資源位置之間的該主通訊通道中至少一個使用該檔案系統之作業系統服務所提供的驗證機制。

8. 如申請專利範圍第 5 項所述之方法，其中該檔案系統係一用於該客戶端應用程式及該伺服器應用程式中至少一個的遠端檔案系統，及在該客戶端應用程式及該資源位置之間的該主通訊通道及在該伺服器應用程式及該資源位置之間的該主通訊通道中至少一個分別使用該遠端檔案系統的掛載(mounting)以分別用於該客戶端應用程式及該伺服器應用程式中至少一個的連線及驗證。

9. 如申請專利範圍第 1 項所述之方法，其中在該客戶端應用程式

及該資源位置之間的該主通訊通道及在該伺服器應用程式及該資源位置之間的該主通訊通道中至少一個使用一驗證的網路通訊協定。

10. 如申請專利範圍第 9 項所述之方法，其中該網路通訊協定係安全通訊端層(SSL)，及儲存於該資源位置的該驗證訊標為統一資源定位器(URL)所識別。

11. 如申請專利範圍第 1 項所述之方法，其中在該產生的驗證訊標儲存於該資源位置之前，已經建立該次通訊通道。

12. 如申請專利範圍第 1 項所述之方法，其中加密在該客戶端應用程式及該資源位置之間的該主通訊通道及在該伺服器應用程式及該資源位置之間的該主通訊通道，及在該客戶端應用程式建立與該伺服器應用程式的該次通訊通道之前，將該產生的驗證訊標儲存於該資源位置。

13. 如申請專利範圍第 1 項所述之方法，其中該客戶端應用程式係一資料庫驅動程式的客戶端元件，及該伺服器應用程式係該資料庫驅動程式的伺服器元件。

14. 如申請專利範圍第 1 項所述之方法，其中該客戶端應用程式由該伺服器應用程式替換，及反之亦然；及在該客戶端應用程式及該資源位置之間的該主通訊通道由在該伺服器應用程式及該資源位置之間的該主通訊通道替換，及反之亦然。

15. 一種驗證系統，其具有運行一客戶端應用程式的一客戶端裝置、一執行一伺服器應用程式的伺服器裝置、一資源位置、一在該客戶端裝置及該資源位置之間的驗證主通訊通道、及一在該伺服器裝置及該資源位置之間的驗證主通訊通道，該系統施行以下步驟：

該客戶端應用程式建立一與該伺服器應用程式的次通訊通道；

該客戶端應用程式經由該次通訊通道提出一請求至該伺服器應用程式，要求授予存取權限；

該伺服器應用程式在該驗證成功後，經由該次通訊通道授予存取權限給該客戶端應用程式；

該系統特徵在於其另外包含施行以下步驟的構件：

該伺服器應用程式啟始將要儲存於該資源位置之一驗證訊標的產生，該客戶端應用程式可經由在該客戶端應用程式及該資源位置之間的該驗證主通訊通道存取該驗證訊標；

該客戶端應用程式經由在該客戶端應用程式及該資源位置之間的該驗證主通訊通道擷取該資源位置的該驗證訊標；

該客戶端應用程式經由該次通訊通道，將該驗證訊標傳回該伺服器應用程式；

該伺服器應用程式藉由檢查該客戶端應用程式傳回該伺服器應用程式的該驗證訊標是否匹配該伺服器應用程式啟始後儲存於該資源位置(103)之該產生的驗證訊標，驗證該客戶端應用程式。

16. 如申請專利範圍第 15 項所述之系統，其中該客戶端應用程式及該伺服器應用程式運行於相同的裝置中。

17. 如申請專利範圍第 15 或 16 項所述之系統，其中該伺服器裝置及該客戶端裝置中至少一個另外包含該資源位置。

18. 一種電腦程式產品，其實施一在一資料處理系統中執行的驗證機制且包含施行如前述申請專利範圍第 1 至 14 項中的任一項所述之系統步驟的電腦程式碼部分。

八、圖式：

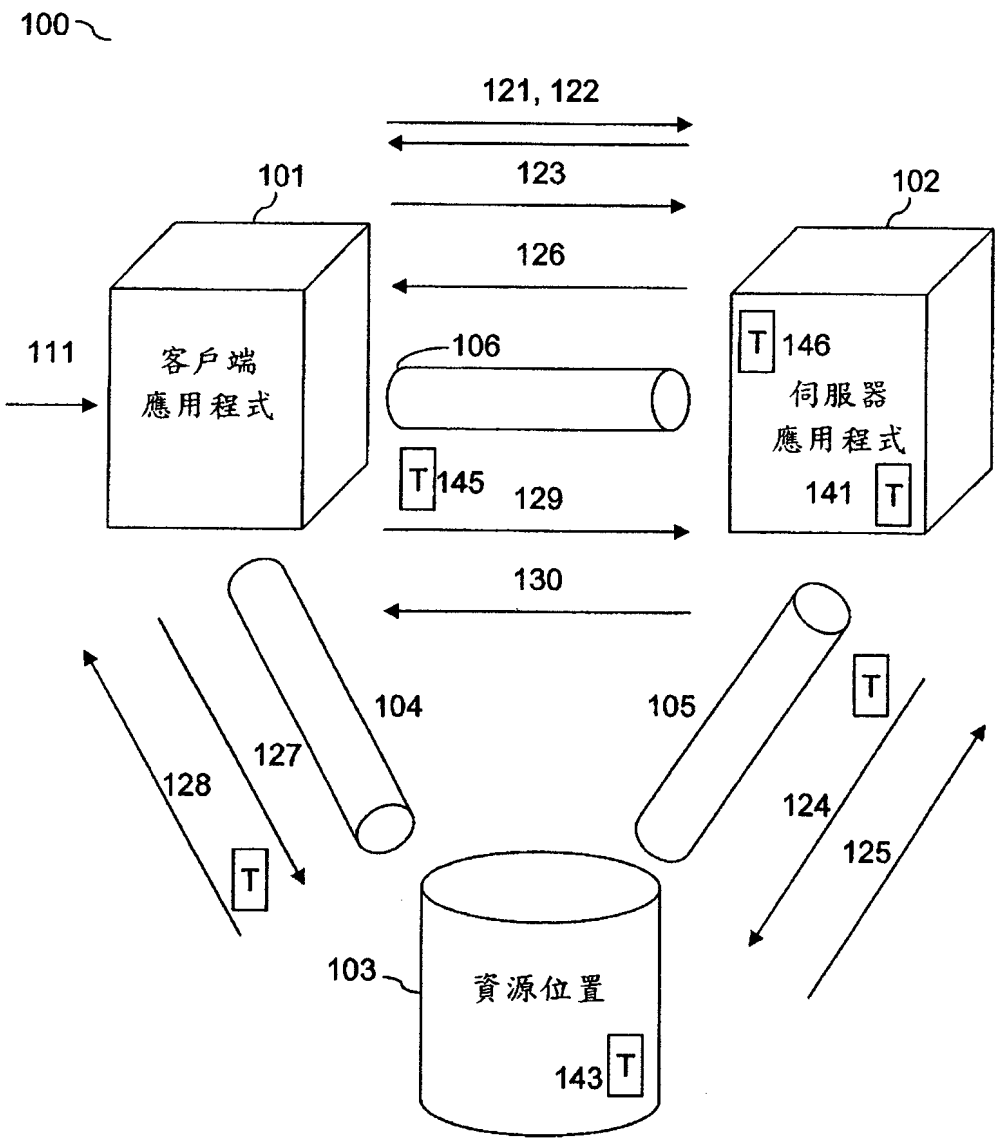

100
121, 122
123
101
102
126
111
客戶端
應用程式
106
T 146
伺服器
應用程式
141 T
T 145
129
130
104
105
T
127
128
124
125
T
103
資源位置
143 T

圖1

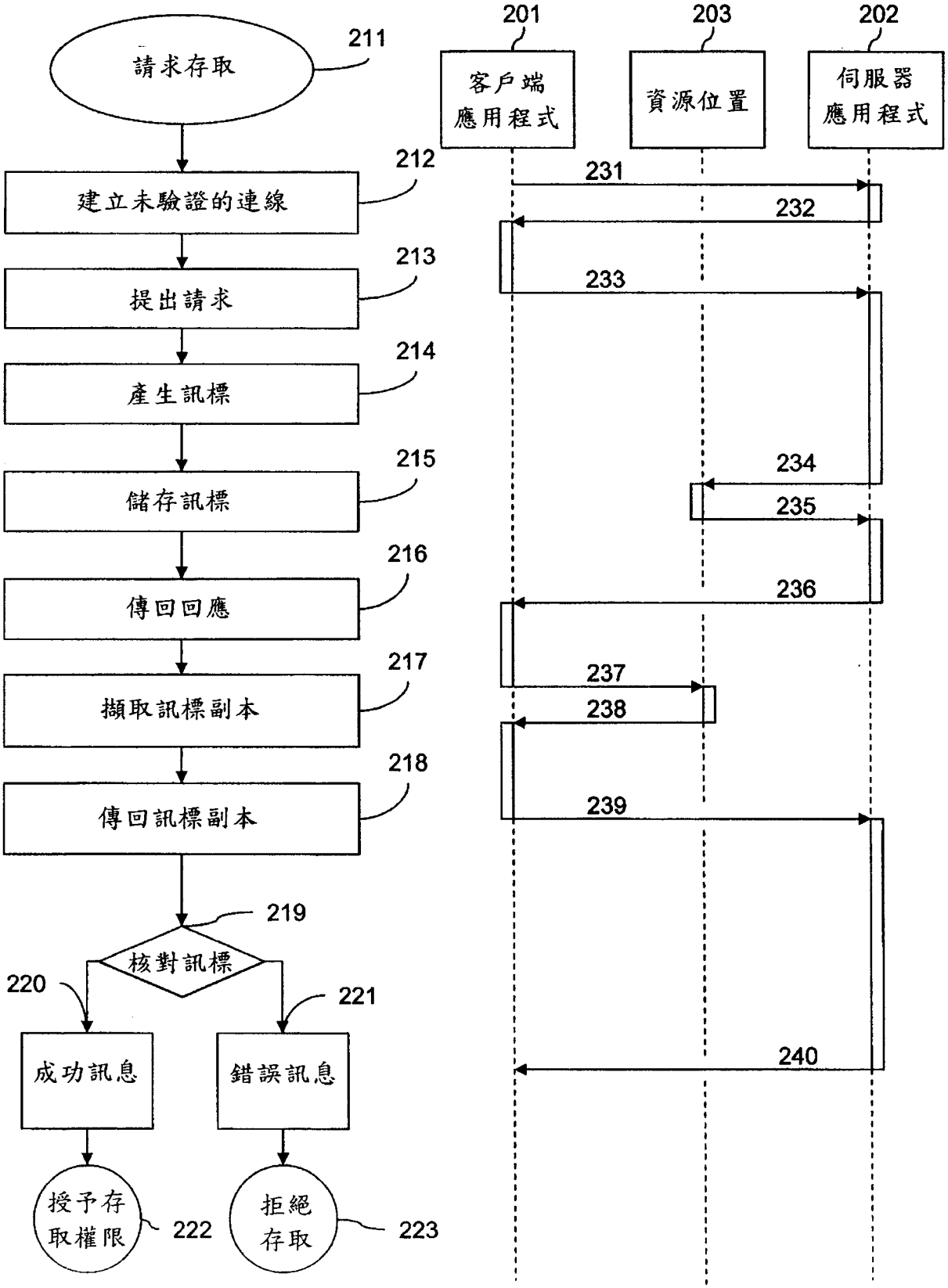

請求存取
211
建立未驗證的連線
212
提出請求
213
產生訊標
214
儲存訊標
215
傳回回應
216
擷取訊標副本
217
傳回訊標副本
218
核對訊標
219
220
221
成功訊息
錯誤訊息
授予存取權限
222
拒絕存取
223
201
客戶端應用程式
203
資源位置
202
伺服器應用程式
231
232
233
234
235
236
237
238
239
240

圖2

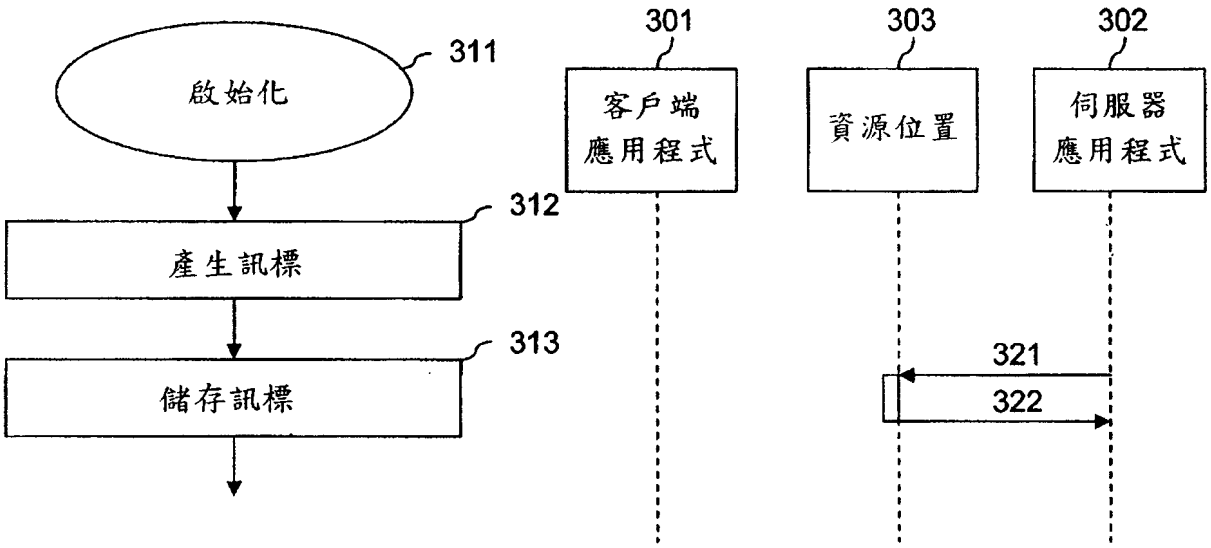

311
啟始化
312
產生訊標
313
儲存訊標
301
客戶端
應用程式
303
資源位置
302
伺服器
應用程式
321
322

圖3

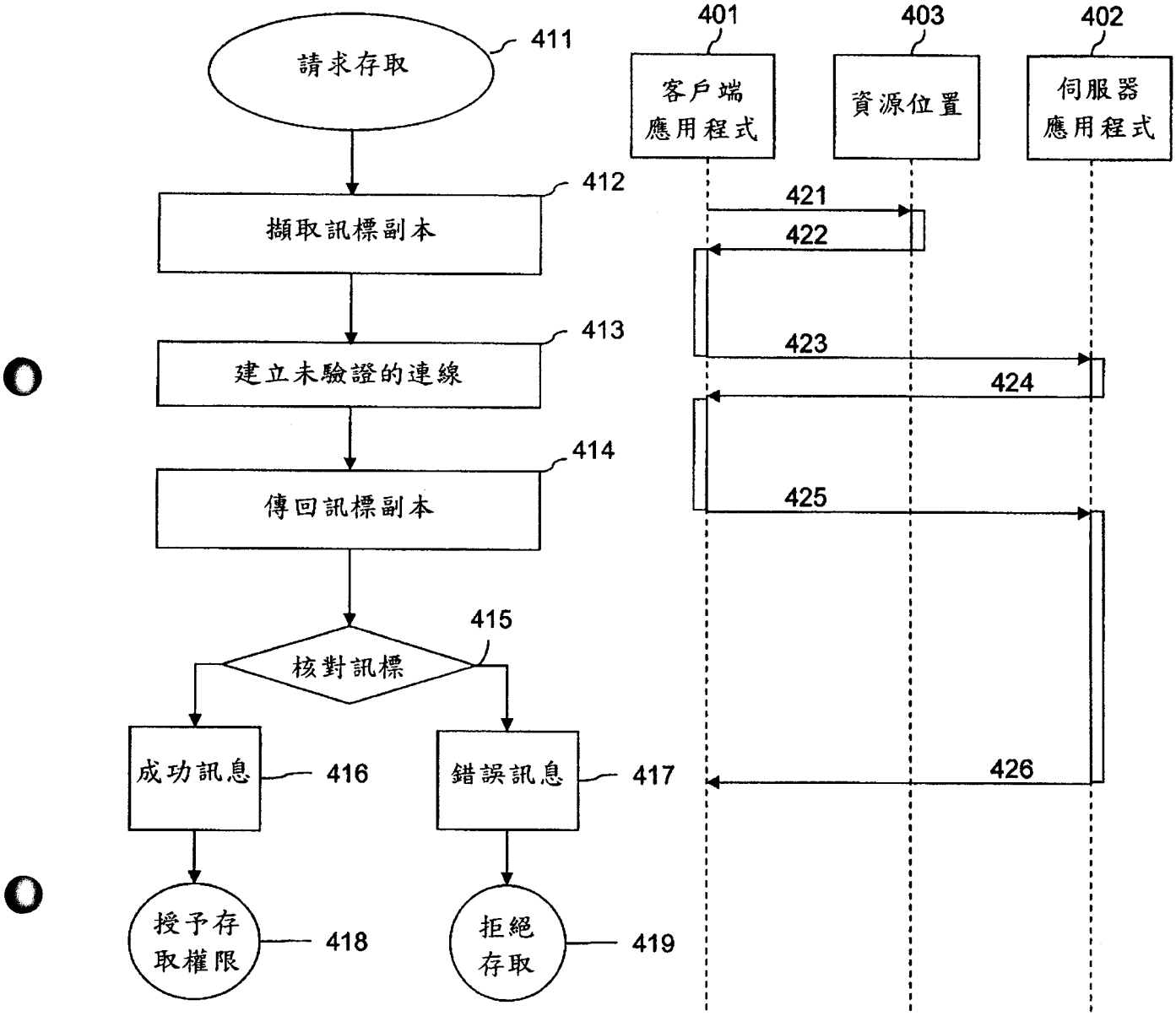

請求存取
411
擷取訊標副本
412
建立未驗證的連線
413
傳回訊標副本
414
核對訊標
415
成功訊息
416
錯誤訊息
417
授予存取權限
418
拒絕存取
419
401
客戶端應用程式
403
資源位置
402
伺服器應用程式
421
422
423
424
425
426

圖4

四、指定代表圖：

(一)本案指定代表圖為：圖 1。

(二)本代表圖之元件符號簡單說明：

100	系統
101	客戶端應用程式
102	伺服器應用程式
103	資源位置
104、105	主通訊通道
106	次通訊通道
141、143	驗證訊標
145、146	驗證訊標副本

五、本案若有化學式時，請揭示最能顯示發明特徵的化學式：無。