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：94147617

※ 申請日期：94.12.2 ※IPC 分類：H04L 9/32 (2006.01)

一、發明名稱：（中文/英文）

用以保護連接暫存器名字識別符設定檔之方法及系統

METHOD AND SYSTEM FOR SECURE BINDING REGISTER NAME IDENTIFIER PROFILE

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）

海瑟 瑪利亞 希頓

HINTON, HEATHER MARIA

國 籍：（中文/英文）

加拿大 CANADA

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. 美國；2004年12月10日；11/010,228

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。

九、發明說明：

【發明所屬之技術領域】

本發明係關於一種改良資料處理系統，且特定言之係關於一種用於多電腦資料傳送之方法及裝置。亦更特定言之，本發明係針對網路電腦系統。

【先前技術】

企業通常需要以使用者友好方式遍及多種網路(包含網際網路)向經授權之使用者提供對受保護資源的安全存取。雖然提供安全驗證機制減小未經授權存取受保護資源之風險，但是彼等驗證機制可成為對受保護資源存取之阻障。使用者通常需要自與一應用相互作用改變至與另一應用相互作用之能力而不考慮保護支持彼等應用之每一特定系統的驗證阻障。

隨著使用者變得更精通，其期望電腦系統協調其行為以使得使用者之負擔減輕。此等類型之期望亦應用於驗證過程。一使用者可假定一旦他或者她已由某電腦系統驗證，則該驗證遍及使用者之工作會話而係有效的，或至少對於一特定時間週期係有效的，而不考慮對於使用者幾乎不可見之各種電腦架構邊界。企業通常試圖實現在其部署之系統之操作特徵中的此等期望，不僅撫慰使用者且亦提高使用者效率，無論使用者效率係關於雇員生產率或是消費者滿意度。

更具體言之，在其中諸多應用具有可經由一共用瀏覽器進行存取之基於Web之使用者介面的當前計算環境中，使

用者期望更多使用者友好性以及對於自一基於Web之應用至另一者之移動的較低或稀少阻障。在本文中，使用者將期望自與在一網際網路域上之一應用相互作用跳至與在另一域上之另一應用相互作用而不考慮保護每一特定域之驗證阻障的能力。然而，即使諸多系統經由易於使用、基於Web之介面提供安全驗證，仍可強制一使用者考慮妨礙使用者越過一組域存取之多個驗證過程。在一給定時間訊框中使一使用者經受多個驗證過程可顯著地影響該使用者之效率。

舉例而言，已使用各種技術來減輕使用者及電腦系統管理者之驗證負擔。此等技術通常經描述為"單一登入"(SSO)過程，因為其具有一共同目的：在一使用者已完成登入操作之後(意即已受到驗證)，隨後並不要求該使用者執行另一驗證操作。因此，目標係在一特定使用者會話期間要求使用者僅完成一個驗證過程。

為降低使用者管理成本且改良企業中的互用性，已建立聯合計算空間。一聯合係堅持某些互用性標準之企業之松耦合聯繫；該聯合相對於該聯合內之使用者之某些計算操作而提供一在彼等企業之中的信任機制。舉例而言，一聯合夥伴可充當使用者之本籍域或識別碼提供者。在相同聯合內之其他夥伴可依賴於使用者之識別碼提供者用於該使用者之驗證憑證之主要管理，例如接受由該使用者之識別碼提供者提供之單一登入符記。

隨著企業移至支持聯合商務相互作用，此等企業應提供

反映在兩個商務之間之增強合作的使用者經驗。如上提及，一使用者可驗證充當識別碼提供者之一方且隨後單一登入充當服務提供者之聯合商務夥伴。與此單一登入功能性相結合，亦應支持額外使用者有效期功能性(諸如帳戶鏈接/去鏈接及單一註銷)。

帳戶鏈接係一種過程，在不同服務提供者處之兩或兩個以上使用者帳戶藉由此過程結合至一單一使用者。此連接可基於使用者之公開識別碼或類似識別符，有時稱作一共用唯一識別符或全局唯一使用者識別符，其易於與一使用者相關聯；此連接可基於一假名(其亦已知為一別名)。

帳戶鏈接係在藉由自由聯盟計劃(Liberty Alliance Project)定義之設定檔內受到支持。根據自由聯盟規格，自由設定檔係用於單一用戶端類型之訊息內容規格及訊息傳送機制規格的組合。自由聯盟規格將此等各種設定檔分組為若干類別。單一登入及聯合設定檔係服務提供者藉由其獲取一來自任一促進單一登入及識別碼聯合之識別碼提供者之驗證判定的彼等設定檔。一識別碼提供者係一實體，其建立、維持且管理關於主要者之識別碼資訊且將主要者驗證提供至與其具有信任關係之其他服務提供者。一服務提供者係一將服務及/或物品提供至主要者之實體，其係一可獲取一聯合識別碼使得代表其執行聯合行為的實體，諸如一個別使用者、一公司或一聯合之某些其他組份。單一註銷設定檔係通知服務提供者及識別碼提供者驗證之會話終止的彼等設定檔。名字註冊設定檔係服務提供

者及識別碼提供者藉由其來指定當彼此關於一主要者通信時將使用之名字識別符的彼等設定檔。

詳言之，自由聯盟計劃已定義一將用於建立帳戶鏈接之"暫存器名字識別符"(RNI)設定檔。暫存器名字識別符設定檔係服務提供者或者識別碼提供者可藉由其來註冊或改變用於一主要者之名字識別符的彼等設定檔。

然而，暫存器名字識別符設定檔並不適於識別使用者至本端帳戶(一帳戶連接操作係基於其)之初始連接。更具體言之，自由聯盟規格提供在一個非常特殊實例中用於安全帳戶鏈接之方案：當自一服務提供者至一識別碼提供者初始化時，在使用者已對於一服務提供者驗證之後，藉此要求該使用者與識別碼提供者進行一會話。藉由在單一登入請求中將元素"聯合"設定為布爾數學的"真"值來初始化此方案；為回應，識別碼提供者將一單一登入回應發送至服務提供者(在其處，使用者已受到驗證)，其又要求甚至當使用者具有一有效會話時服務提供者能夠容納一單一登入回應。

此方案提出若干實施問題。舉例而言，其可導致使用者之會話憑證之不適當重設，因為其必須立即重設以指示使用者已經由一來自識別碼提供者之單一登入操作而受到驗證替代於與服務提供者直接驗證，意即替代於可在單一登入操作之前已完成之驗證方法；若使用者之會話憑證並未適當地重設，則已潛在損害安全性，因為使用者可具有由服務提供者授權之用於直接驗證使用者而並非經授權用於

已執行一單一登入操作之使用者的行為。

一旦此初始聯合操作完成(由服務提供者連接/重連接，及僅由識別碼提供者重連接)，則自由聯盟規格描述之"暫存器名字識別符"設定檔僅考慮帳戶連接/重連接。因此，具有其中一企業可實施一暫存器名字識別符設定檔使得該暫存器名字識別符設定檔充分識別一使用者至一本端帳戶之初始連接(帳戶鏈接操作係基於其)的方法及系統係有利的。

【發明內容】

本文提出一種方法、一種系統、一種裝置及一種電腦程式產品，其用於改良在一聯合計算環境中之暫存器名字識別符設定檔使得增強暫存器名字識別符設定檔在聯合計算環境內的兩個聯合實體(諸如一識別碼提供者與一服務提供者)之間更安全地連接。在第一聯合實體將一用於一主要者之暫存器名字識別符請求發送至第二聯合實體之後，該第二聯合實體執行一用於該主要者之驗證操作。回應於成功地完成該驗證操作，該第二聯合實體註冊或修正一已自接收之暫存器名字識別符請求擷取之用於該主要者的名字識別符。

【實施方式】

一般而言，可包括或係關於本發明之設備包括各種各樣的資料處理技術。因此，作為背景，在更詳細描述本發明之前描述在一分散式資料處理系統內的硬體組件及軟體組件之一典型組織。

現參看諸圖，圖1A描述一資料處理系統典型網路，其中之每一者可實施本發明。分散式資料處理系統100含有網路101，其係一可用於在各種設備與在分散式資料處理系統100內連接起來的電腦之間提供通信鏈路的媒體。網路101可包括永久性連接如導線或光纖電纜，或者經由電話或無線通信做出之臨時連接。在已描述之實例中，伺服器102及伺服器103與儲存單元104一起連接至網路101。另外，用戶端105-107亦連接至網路101。用戶端105-107及伺服器102-103可由多種計算設備來表示，諸如大型電腦、個人電腦、個人數位助理(PDA)等等。分散式資料處理系統100可包括額外伺服器、用戶端、路由器、其它設備及未展示之點對點架構。

在描述之實例中，分散式資料處理系統100可包括具有網路101之網際網路，其表示使用彼此通信之各種協定的網路及閘道器之世界範圍內的聚集，該等協定諸如LDAP(輕型目錄存取協定)、TCP/IP(傳送控制協定/網際網路協定)、HTTP(超文字傳送協定)等等。當然，分散式資料處理系統100亦可包括若干不同類型之網路如企業內部網路、區域網路(LAN)或廣域網路(WAN)。舉例而言，伺服器102直接支持用戶端109及網路110，其併入有無線通信鏈路。網路賦能之電話111經由無線鏈路112連接至網路110，且PDA 113經由無線鏈路114連接至網路110。電話111及PDA 113亦可使用諸如Bluetooth™無線技術之適當技術越過無線鏈路115而在其間直接傳送資料，以建立所謂

的個人區域網路或個人特別網路。以一類似方式，PDA 113可經由無線通信鏈路116將資料傳送至PDA 107。

本發明可實施於多種硬體平臺及軟體環境。圖1A希望作為異質計算環境之一實例而非作為本發明之架構限制。

現參看圖1B，一圖式描述一資料處理系統之典型電腦架構，諸如圖1A中所示，其中可實施本發明。資料處理系統120含有連接至內部系統匯流排123之一或多個中央處理單元(CPU)122，其互連隨機存取記憶體(RAM)124、唯讀記憶體126及輸入/輸出配接器128，其支持各種I/O設備如印表機130、碟片單元132、或者未展示的其它設備如音訊輸出系統等等。系統匯流排123亦將提供存取之通信配接器134連接至通信鏈路136。使用者介面配接器148連接各種使用者設備如鍵盤140及滑鼠142，或者未展示之其它設備如觸控螢幕、尖筆(stylus)、麥克風等等。顯示配接器144將系統匯流排123連接至顯示設備146。

普通熟習此項技術者應瞭解，圖1B中之硬體可視系統實施而變化。舉例而言，系統可具有一或多個處理器，諸如一基於Intel® Pentium®之處理器及一數位訊號處理器(DSP)、以及一或多個類型之揮發性及非揮發性記憶體。附加至或替代於圖1B中描述之硬體可使用其它周邊設備。描述之實例並非意謂包含相對於本發明之架構限制。

除能夠在多種硬體平臺上實施以外，本發明可在多種軟體環境中實施。可使用典型作業系統來控制在每一資料處理系統內之程式執行。舉例而言，一設備可運行一Unix®

作業系統，而另一設備含有一簡單Java®運行時間環境。一代表性電腦平臺可包括一瀏覽器，其係一用於以多種格式存取超文字文獻之熟知軟體應用，諸如圖形檔案、字處理檔案、可延伸性標記語言(XML)、超文字標記語言(HTML)、掌上型設備標記語言(HDML)、無線標記語言(WML)及各種其它格式及類型之檔案。亦請注意，圖1A所示之分散式資料處理系統係涵蓋為完全能夠支持多種點對點子網路及點對點服務。

現參看圖1C，一資料流程圖說明當一用戶端試圖在伺服器存取一受保護資源時所使用的典型驗證過程。如說明，在用戶端工作站150處之使用者試圖經由該使用者之在用戶端工作站上執行之網路瀏覽器經一電腦網路存取伺服器151上的受保護資源。一受保護或受控的資源係一為其而使存取受控或受限制的資源(一應用、一物件、一文獻、一頁、一檔案、可執行碼、或其它計算資源、通信類型資源等等)。一受保護資源由一個一致資源定位器(URL)識別，或更通常地，其由一僅可由已驗證及/或經授權之使用者存取的一致資源識別符(URI)識別。電腦網路可為網際網路、企業內部網路、或其它網路，如圖1A或圖1B中所示，且伺服器可為web應用伺服器(WAS)、伺服器應用、servlet過程(servlet process)或其類似物。

當使用者請求一伺服器側之受保護資源時初始化該過程，諸如在域"ibm.com"內的網頁(步驟152)。術語"伺服器側"及"用戶端側"係指分別在一網路環境內之伺服器或用

戶端處的行為或實體。網路瀏覽器(或者相關聯之應用或applet(Java之小程式))產生一發送至管理域"ibm.com"之網路伺服器的HTTP請求(步驟153)。術語"請求"及"回應"應理解為包含適用於包含於一特定操作中之資訊(諸如訊息、通信協定資訊或其它相關聯之資訊)之傳送的資料格式化。

伺服器判定其並非具有用於用戶端之有效會話(步驟154)，因此該伺服器在伺服器與用戶端之間初始化並完成一SSL(安全套接層)會話之建立(步驟155)，其要求在用戶端與伺服器之間之資訊的多個傳送。在建立一SSL會話之後，在該SSL會話內傳送隨後之通信訊息；歸因於該SSL會話內之加密的通信訊息，任一機密資訊仍為安全的。

然而，在允許使用者存取受保護資源之前，該伺服器需要判定該使用者之識別碼，因此該伺服器藉由向用戶端發送某類型之驗證查問來要求該使用者執行一驗證過程(步驟156)。驗證查問可以各種格式，諸如一HTML形式。該使用者接著提供請求或要求之資訊(步驟157)，諸如連同一相關聯之通行碼或其它形式之機密資訊的使用者名字或其它類型之使用者識別符。

將驗證回應資訊發送至該伺服器(步驟158)，在該點處該伺服器例如藉由擷取先前提交之註冊資訊及將提出之驗證資訊與使用者之儲存資訊匹配來驗證使用者或用戶端(步驟159)。假定該驗證係成功的，則建立一用於驗證之使用者或者用戶端的有效會話。該伺服器建立一用於該用戶

端之會話識別符，且在該會話內之來自該用戶端之任何隨後請求訊息將伴有該會話識別符。

該伺服器接著擷取起初請求之網頁且將一HTTP回應訊息發送至該用戶端(步驟160)，進而滿足該使用者對於受保護資源之原始請求。在彼點處，該使用者可藉由在一瀏覽器視窗內點擊一超文字鏈接而請求在"ibm.com"內的另一頁(步驟161)，且該瀏覽器將另一HTTP請求訊息發送至伺服器(步驟162)。在彼點處，伺服器認為該使用者具有一有效會話(步驟163)，因為該使用者之會話識別符在該HTTP請求訊息中返回至伺服器，且伺服器在另一HTTP回應訊息中將請求之網頁返回發送回至用戶端(步驟164)。雖然圖1C描述一典型先前技術過程，但是應注意可描述其它替代性會話狀態管理技術，諸如URL重寫或使用cookie以識別具有有效會話之使用者，其可包括使用用於提供驗證之證明的相同cookie。

現參看圖1D，一網路圖說明一可實施本發明之典型基於Web的環境。在此環境中，位於用戶端171之瀏覽器170之使用者需要在DNS域173中之web應用伺服器172或在DNS域175中之web應用伺服器174上存取一受保護資源。

以類似於圖1C中所示之方式，一使用者可在諸多域中之一者處請求一受保護資源。與圖1C相比，其展示一特定域處之僅一單一伺服器，圖1D中之每一域具有多個伺服器。詳言之，每一域可具有一相關聯之驗證伺服器176及177。

在此實例中，在用戶端171發佈對域173處之受保護資源

的請求之後，web應用伺服器172判定其並非具有用於用戶端171之有效會話，且其請求驗證伺服器176對用戶端171執行一適當驗證操作。驗證伺服器176將驗證操作之結果通信至web應用伺服器172。若使用者(或代表該使用者之瀏覽器170或用戶端171)受到成功地驗證，則web應用伺服器172建立一用於用戶端171之會話並返回請求之受保護資源。通常，一旦使用者由驗證伺服器驗證，則一cookie可經設定且儲存於瀏覽器中之cookie快取記憶體中。圖1D僅係一方式之一實例，其中可在多個伺服器之中共用一域之處理資源，特定言之執行驗證操作。

以一類似方式，在用戶端171發佈對域175處之受保護資源的請求之後，驗證伺服器177對用戶端171執行一適當驗證操作，在其後web應用伺服器174建立一用於用戶端171之會話且返回請求之受保護資源。因此，圖1D說明用戶端171在不同域中可具有多個同時發生的會話然而要求其完成建立彼等同時發生之會話的多個驗證操作。

現參看圖1E，一方塊圖描述可要求來自一使用者之多個驗證操作之典型線上交易的一實例。再次參看圖1C及圖1D，如圖1C中所示，可要求使用者在獲得對於受控資源之存取之前完成一驗證操作。雖然在圖1C中並未展示，但是可在伺服器151上布署一驗證管理器以擷取且使用受到要求以驗證一使用者的使用者資訊。如圖1D中所示，一使用者在不同域173及175內可具有多個當前會話，且雖然其並未在圖1D中展示，但是每一域可使用一驗證管理器以替

代於驗證伺服器或附加至驗證伺服器。以一類似方式，圖1E亦描述一組域，其之每一域支持某類型之驗證管理器。圖1E說明當存取要求使用者完成一用於每一域之驗證操作的多個域時，使用者可經歷的某些困難。

使用者190可在ISP域191處註冊，其可支持為相對於域191完成交易之目的而驗證使用者190的驗證管理器192。ISP域191可為一提供網際網路連接服務、電子郵件服務及可能的其它電子貿易服務之網際網路服務提供者(ISP)。或者，ISP域191可為一由使用者190頻繁存取之網際網路入口。

類似地，域193、195及197表示典型網路服務提供者。政府域193支持驗證用於完成各種政府相關交易之使用者的驗證管理器194。銀行域195支持驗證用於用一線上銀行完成交易之使用者的驗證管理器196。電子貿易域197支持驗證用於完成線上購買之使用者的驗證管理器198。

如先前提及，當使用者試圖藉由存取不同域處之資源而在網際網路或全球資訊網內自一個域移至另一域時，一使用者可經受多個使用者驗證請求或要求，其可顯著地減慢該使用者越過一組域之進程。將圖1E用作一例示性環境，使用者190可包含於與電子貿易域197之複雜的線上交易中，其中該使用者試圖購買一線上服務，該服務限於至少18歲的使用者及具有一有效駕駛執照、一有效信用卡及一美國銀行帳戶的使用者。此線上交易可涉及域191、193、195及197。

通常，一使用者並不維持一識別碼及/或在參與一典型線上交易之每一域內的屬性。在此實例中，使用者190可註冊他或她之識別碼及該使用者之ISP，但是為完成該線上交易，亦要求該使用者對域193、195及域197進行驗證。若該等域中之每一者並不維持用於該使用者之識別碼，則該使用者之線上交易可失敗。即使每一域可驗證該使用者，亦不保證不同域可在其間傳送資訊以完成使用者之交易。

考慮到某當前技術之先前簡要描述，剩餘圖式之描述係關於可操作本發明之聯合電腦環境。然而，在更詳細地論述本發明之前，引入某些術語。

術語

術語"實體"或"方"通常係指一組織、一個體、或代表一組織、一個體或另一系統而操作的系統。術語"域"意謂一網路環境內之額外特徵，但是可交換地使用術語"實體"、"方"及"域"。舉例而言，術語"域"亦可係指一DNS(域名系統)域，或更通常地，其係指一包括對於外部實體呈現為一邏輯單元之各種設備及應用的資料處理系統。

術語"請求"及"回應"應理解為包含適於包含於一特定操作中之資訊之傳送的資料格式化，諸如訊息、通信協定資訊或其它相關聯之資訊。一受保護資源係一為其而使存取受控或受限制的資源(一應用、一物件、一文獻、一頁、一檔案、可執行碼、或其它計算資源、通信類型資源等等)。

一符記提供一成功操作之直接跡象且由執行該操作之實體產生，例如，在一成功驗證操作之後產生的驗證符記。一Kerberos符記係可用於本發明中之驗證符記之一實例。可在網際網路工程工作小組(IETF)請求說明(RFC)1510, 09/1993之Kohl等人的"The Kerberos Network Authentication Service (V5)"中找到更多關於Kerberos之資訊。

一聲明提供某行為之間接跡象。聲明可提供識別碼、驗證、屬性、授權決策、或其它資訊及/或操作之間接跡象。一驗證聲明提供藉由並非驗證服務但傾聽驗證服務之實體的驗證間接跡象。

一安全宣示標記語言(SAML)聲明係一可用於本發明內之可能的聲明格式之一實例。結構化資訊標準推動組織(OASIS)已公佈SAML，該組織係非盈利的全球性協會。SAML係在委員會說明書01, 05/31/2002之"Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML)"中描述如下：

安全宣示標記語言(SAML)係用於交換安全資訊之基於XML的構架。此安全資訊以關於主體聲明之形式表現，其中一主體係一具有一在某安全域中之識別碼的實體(人或電腦)。一主體之一典型實例係一人，藉由其在一特定網際網路DNS域中之電子郵件位址來識別。聲明可傳達關於由主體執行之驗證行為的資訊、主體之屬性及關於是否允許主體存取某些資源之授權決策。聲明係表示為XML構造

並且具有一巢套結構，藉此一單一聲明可含有關於驗證、授權及屬性之若干不同內部陳述。注意含有驗證陳述之聲明僅描述先前發生之驗證的行為。由SAML權限發佈聲明，即驗證權限、屬性權限及策略決策點。SAML定義一協定，用戶端可藉由該協定自SAML權限請求聲明且自其獲得一回應。此由基於XML之請求及回應訊息格式組成之協定可結合至諸多不同之潛在通信及傳送協定；SAML當前定義一結合，其經HTTP結合至SOAP。SAML權限在創建其回應中可使用各種資訊資源，諸如外部策略儲存及作為請求中之輸入接收的聲明。因此，雖然用戶端總消費聲明，但是SAML權限可係聲明之產生者及消費者。

SAML說明書陳述聲明係一供應由發佈者做出之一或多個陳述的資訊封包。SAML允許發佈者做出三種不同種類之聲明陳述：驗證，其中指明之主體在特定時間由特定構件驗證；授權，其中允許指明之主體存取指明之資源的請求已受到授予或拒絕；及屬性，其中指明之主體係與供應之屬性相關聯。如下進一步論述，當必需時可將各種聲明格式轉譯為其它聲明格式。

驗證係驗證由一使用者提供或者代表一使用者之一組憑證之過程。藉由驗證使用者知道之某物、使用者具有之某物或使用者作為之某物(意即某些關於使用者之實體特徵)來完成驗證。使用者知道之某物可包括一共用機密如使用者之通行碼，或藉由驗證僅為一特定使用者所知的某物如使用者之密碼編譯密鑰。使用者具有之某物可包括智能卡

或硬體符記。關於使用者之某實體特徵可包括一生物統計輸入如指紋或視網膜圖像。

一驗證憑證係用於各種驗證協定中之一組查問/回應資訊。舉例而言，一使用者名字及通行碼之組合係最常見形式之驗證憑證。其它形式之驗證憑證可包括各種形式之查問/回應資訊，公用密鑰基礎建設(PKI)證明、智能卡、生物統計等等。一驗證憑證與驗證聲明係不同的：驗證憑證由使用者提出而作為具有一驗證伺服器或服務之驗證協定序列的一部分；且驗證聲明係關於使用者之驗證憑證之成功提出及驗證的當必須時隨後在實體之間傳送的陳述。

暫存器名字識別符設定檔

如上提及，自由聯盟計劃已定義將用於建立帳戶鏈接之暫存器名字識別符設定檔。根據先前技術之自由聯盟規格，自由設定檔係用於單一用戶端類型之一訊息內容規格與一訊息傳送機制規格之組合。暫存器名字識別符設定檔係服務提供者或識別碼提供者可藉由其註冊或改變用於一主要者之名字識別符的彼等設定檔，其已在圖2A及2B中說明。

現參看圖2A，一資料流程圖描述一如在先前技術之自由聯盟規格內定義之由識別碼提供者初始化之基於HTTP重定向的暫存器名字識別符設定檔。由於對於先前技術之自由聯盟規格之實施特殊的多種原因，識別碼提供者可改變(意即註冊)已由識別碼提供者指派至一主要者的名字識別符，其已知為"<lib: IDPProvidedNameIdentifier>"；識別

碼提供者以圖2A中所示之方式將新近指派之名字識別符傳輸至服務提供者。

藉由將HTTP重定向訊息(具有狀態/原因碼"302"之HTTP回應訊息)發送至用戶端(亦已知為使用者代理，諸如網路瀏覽器應用)而在識別碼提供者處開始基於HTTP重定向之暫存器名字識別符設定檔(步驟202)。基於HTTP重定向之暫存器名字識別符設定檔不可由識別碼提供者自行初始化；其必須由某類型之訊息或在識別碼提供者與另一實體(使用者代理或服務提供者)之間的相互作用觸發，雖然該訊息並未在圖2A中展示。重定向訊息將用戶端重定向至在服務提供者處之暫存器名字識別符服務之適當位置，該位置例如藉由在重定向訊息之"位置"標頭內的一致資源識別符(URI)來識別。重定向訊息之"位置"HTTP標頭亦包括一查詢組件，其例如附加至URI且在URI內用一"?"字元區分，其含有如在先前技術之自由聯盟規格內定義之"<lib: RegisterNameIdentifierRequest>"協定訊息。

回應於自識別碼提供者接收重定向訊息，用戶端如由來自識別碼提供者之HTTP重定向訊息中的URI指示而將一HTTP Get訊息發送至服務提供者處之暫存器名字識別符服務(步驟204)。以此方式，用戶端存取服務提供者處之暫存器名字識別符服務，因為在HTTP Get訊息中之URI仍然含有附加之"<lib: RegisterNameIdentifierRequest>"訊息。因此，服務提供者處理暫存器名字識別符請求訊息(步驟206)，進而註冊由識別碼提供者指派至主要者之名字識別

符。

在處理暫存器名字識別符請求訊息之後，服務提供者處之暫存器名字識別符服務藉由將一HTTP重定向訊息(具有狀態/原因碼"302"之HTTP回應訊息)發送至用戶端而回應(步驟208)。重定向訊息使用由識別碼提供者提供之返回URI將用戶端重定向至識別碼提供者，該返回URI在暫存器名字識別符請求訊息內的"RegisterNameIdentifierServiceReturnURL"中繼資料元素中。返回URI在重定向訊息之"位置"HTTP標頭中指明。重定向訊息之"位置"HTTP標頭亦包括一查詢組件，其例如附加至URI且在該URI內用一"?"字元區分，其含有如在先前技術自由聯盟規格內定義之"<lib: RegisterNameIdentifierResponse>"協定訊息。

回應於自服務提供者接收重定向訊息，用戶端如由來自服務提供者之HTTP重定向訊息中的URI指示而將一HTTP Get訊息發送至識別碼提供者(步驟210)，進而結束過程。因為自用戶端至識別碼提供者之HTTP Get訊息中的URI仍然含有附加之"<lib: RegisterNameIdentifierResponse>"訊息，所以用戶端初始化識別碼提供者處之暫存器名字識別符操作之完成。如上提及，基於HTTP重定向之暫存器名字識別符設定檔不可由識別碼提供者自行初始化且必須由某類型之訊息或在識別碼提供者與另一實體(使用者代理或服務提供者)之間的相互作用觸發；因此，可在識別碼提供者接收暫存器名字識別符回應訊息之後完成在圖2A中並未展示之額外處理步驟。

現參看圖2B，一資料流程圖描述一如在先前技術自由聯盟規格內定義之由服務提供者初始化之基於HTTP重定向的暫存器名字識別符設定檔。由於對於先前技術自由聯盟規格之實施特殊的多種原因，服務提供者可改變(意即註冊)已由服務提供者指派至一主要者的名字識別符，其已知為"<lib: SPProvidedNameIdentifier>"；服務提供者以圖2B中所示之方式將新近指派之名字識別符傳輸至識別碼提供者。當識別碼提供者與服務提供者關於特定主要者通信時，服務提供者提供之名字識別符係服務提供者期望識別碼提供者使用之名字識別符；直至服務提供者向識別碼提供者註冊一服務提供者提供之名字識別符為止，識別碼提供者當係指特定主要者時將繼續使用當前指派之識別碼提供者提供的名字識別符。

藉由將HTTP重定向訊息(具有狀態/原因碼"302"之HTTP回應訊息)發送至用戶端(亦已知為使用者代理，諸如網路瀏覽器應用)而在服務提供者處開始基於HTTP重定向之暫存器名字識別符設定檔(步驟222)。基於HTTP重定向之暫存器名字識別符設定檔可由服務提供者自行初始化；其它可能之訊息或在服務提供者與另一實體(使用者代理或識別碼提供者)之間的相互作用在初始化此過程之前未在圖2B中展示。重定向訊息將用戶端重定向至在服務提供者處之暫存器名字識別符服務之適當位置，該位置例如藉由在重定向訊息之"位置"標頭內的URI來識別。重定向訊息之"位置"HTTP標頭亦包括一查詢組件，其例如附加至URI且

在URI內用一"?"字元區分，其含有如在先前技術自由聯盟規格內定義之"<lib: RegisterNameIdentifierRequest>"協定訊息。

回應於自服務提供者接收重定向訊息，用戶端如由來自服務提供者之HTTP重定向訊息中的URI指示而將一HTTP Get訊息發送至識別碼提供者處之暫存器名字識別符服務(步驟224)。因為HTTP Get訊息中之URI仍然含有附加之"<lib: RegisterNameIdentifierRequest>"訊息，所以用戶端以此方式存取識別碼提供者處之暫存器名字識別符服務。因此，識別碼提供者處理暫存器名字識別符請求訊息(步驟226)，進而註冊由服務提供者提供之名字識別符。

在處理暫存器名字識別符請求訊息之後，識別碼提供者處之暫存器名字識別符服務藉由將一HTTP重定向訊息(具有狀態/原因碼"302"之HTTP回應訊息)發送至用戶端而回應(步驟228)。重定向訊息例如使用由服務提供者在暫存器名字識別符請求訊息內提供之返回URI將用戶端重定向至服務提供者。返回URI在重定向訊息之"位置"HTTP標頭中指明。重定向訊息之"位置"HTTP標頭亦包括一查詢組件，其例如附加至URI且在該URI內用一"?"字元區分，其含有如在先前技術自由聯盟規格內定義之"<lib: RegisterNameIdentifierResponse>"協定訊息。

回應於自識別碼提供者接收重定向訊息，用戶端如來自識別碼提供者之HTTP重定向訊息中的URI指示而將一HTTP Get訊息發送至服務提供者(步驟230)，進而結束過

程。因為自用戶端至服務提供者之HTTP Get訊息中的URI仍然含有附加之"<lib: RegisterNameIdentifierResponse>"訊息，所以用戶端初始化服務提供者處之暫存器名字識別符操作之完成。可在服務提供者接收暫存器名字識別符回應訊息之後完成在圖2B並未展示之額外處理步驟。

如上相對於圖2A及圖2B論述，暫存器名字識別符設定檔係服務提供者可藉由其請求註冊用於一主要者之名字識別符或者識別碼提供者或識別碼提供者可藉由其根據先前技術自由聯盟規格改變用於一主要者之名字識別符的彼等設定檔。

由先前技術自由聯盟規格定義之暫存器名字識別符設定檔具有兩個協定實施例：基於HTTP重定向之實施例及一基於SOAP/HTTP之實施例。如上提及，在具有基於HTTP重定向之連接的情況下，希望調用暫存器名字識別符之實體或方必須等待一自使用者傳入之HTTP請求；換言之，基於HTTP重定向之暫存器名字識別符設定檔不可自行初始化。因此，將暫存器名字識別符資料流插入HTTP回應中，例如包括在完成一HTTP GET且返回控制以允許滿足初始HTTP請求之前初始化基於HTTP重定向之進一步GET。

在此方案內之暫存器名字識別符資料流之初始化經結合至初始化實體或一方處之使用者。因此，若暫存器名字識別符設定檔自識別碼提供者觸發，則在一有效範疇內觸發此資料流，驗證會話用於識別碼提供者處之使用者。然

而，暫存器名字識別符設定檔並不要求使用者驗證或單一登入至暫存器名字識別符設定檔範疇之服務提供者。同樣地，具有一暗示的假定：若此等資料流係自一服務提供者調用，則該使用者對識別碼提供者而受到驗證且因此執行至服務提供者之單一登入；因為先前技術自由聯盟規格並不要求服務提供者放棄權利以驗證使用者(甚至在聯合之後)，所以此係一錯誤假定。

在任一方案中，不具有如在識別碼(服務)提供者處初始化之使用者之暫存器名字識別符請求至如在服務(識別碼)提供者處已知之使用者的連接。此意謂並未保證該請求實際上用於正執行之使用者；另外，並未保證請求不重發或另外由使用者或惡意方濫用。

增強的暫存器名字識別符設定檔

本發明藉由要求使用者在兩方(意即識別碼提供者及服務提供者)皆具有有效會話而解決如在自由聯盟規格中描述之暫存器名字識別符設定檔中的以上提及之不足，以完成基於HTTP重定向之暫存器名字識別符流。如下文中相對於圖3A及圖3B更詳細地說明，此方法要求一使用者(大概係為其發生暫存器名字識別符操作的主要者)在暫存器名字識別符操作期間對識別碼提供者及服務提供者進行驗證(或執行一單一登入操作)。雖然在圖3A及圖3B內說明之例示性實施例使用基於HTTP之通信，但是本發明並不限於基於HTTP的通信，且可使用其它通信協定。

現參看圖3A，一資料流程圖描述一增強的基於HTTP重

定向之暫存器名字識別符(RNI)設定檔，其包括一由識別碼提供者根據本發明之一實施例初始化之普遍驗證步驟。以類似於圖2A中展示之方式，圖3A描述一過程，識別碼提供者可藉由此過程在選定之服務提供者處改變(意即註冊)已由識別碼提供者指派至一主要者的名字識別符，已知為"<lib: IDPProvidedNameIdentifier>"，其可因為多種特殊實施原因而發生。然而，如下文中論述，圖3A中所示之過程與圖2A中所示之過程的不同之處在於包括一額外驗證步驟。

用於此資料流之先決條件係使用者已鏈接識別碼提供者與服務提供者處之使用者帳戶(步驟302)且使用者已對於識別碼提供者而受到驗證(步驟304)。在步驟302中，要求僅係至少"<lib: IDPProvidedNameIdentifier>"已受到設定。本發明並未要求在處理中之此點處存在"<lib: SPProvidedNameIdentifier>"。在步驟304中，要求僅係使用者在某先前時間點處已對於識別碼提供者而受到驗證且當前具有與識別碼提供者之有效會話。本發明並未要求建立此會話之原因；舉例而言，其並未要求因為除執行暫存器名字識別符設定檔以外之某目的建立此會話，亦未要求為執行暫存器名字識別符設定檔之目的而明確地建立會話。

藉由將HTTP重定向訊息(具有狀態/原因碼"302"之HTTP回應訊息)發送至用戶端(亦已知為使用者代理，諸如網路瀏覽器應用)而在服務提供者處開始增強的基於HTTP重定

向之暫存器名字識別符設定檔(步驟306)。此訊息可已由若干不同情況觸發，諸如使用者明確請求重設其識別符，或識別碼提供者已設定某基於管理人之觸發，或各種其它類似事件。重定向訊息將用戶端重定向至在服務提供者處之暫存器名字識別符服務之適當位置，該位置例如藉由在重定向訊息之"位置"標頭內的URI來識別。重定向訊息之"位置"HTTP標頭亦包括一查詢組件，其例如附加至URI且在URI內用一"?"字元區分，其含有"<lib: RegisterNameIdentifierRequest>"協定訊息。

回應於自識別碼提供者接收重定向訊息，用戶端如由來自識別碼提供者之HTTP重定向訊息中之URI指示而將HTTP Get訊息發送至服務提供者處之暫存器名字識別符服務(步驟308)。因為在HTTP Get訊息中之URI仍然含有附加之"<lib: RegisterNameIdentifierRequest>"訊息，所以用戶端以此方式存取服務提供者處之暫存器名字識別符服務。

與圖2A中所示之過程相比，服務提供者對使用者、用戶端或使用者代理執行一驗證操作(步驟310)；可假定已要求使用者/用戶端完成對識別碼提供者之驗證操作。若該驗證操作在步驟310並未成功地完成，則服務提供者可立即將一失敗回應返回至識別碼提供者，進而結束該過程。

在步驟310中，要求使用者/用戶端完成一額外驗證操作(意即除識別碼提供者已要求之任一驗證操作以外)，使得服務提供者可保證接收之暫存器名字識別符請求係連接的或可信的；另外，服務提供者可能不可保證接收之暫存器

名字識別符請求訊息並未源自一惡意使用者/系統，且服務提供者不可保證用戶端正執行相關聯之端使用者的RNI請求。一般而言，允許任一隨機使用者載運任一其他隨機使用者之RNI請求並非較佳之實踐。使用本發明，識別碼提供者及服務提供者處之驗證或單一登入之迫使作為暫存器名字識別符設定檔之部分而幫助保證識別碼提供者及服務提供者處之使用者至RNI請求的安全連接受到維持。

在任一狀況下，若服務提供者處之使用者之會話已存在，則不要求服務提供者建立新的會話；其可選擇依賴於預先存在之會話。然而亦應注意，在其中一使用者可具有與單一服務提供者相關聯之多個識別碼提供者的方案中，服務提供者可選擇重建使用者之會話，進而保證在其內執行暫存器名字識別符設定檔之會話明確連接至已初始化暫存器名字識別符之識別碼提供者。

假定在步驟310中成功地完成驗證操作，服務提供者接著處理暫存器名字識別符請求訊息(步驟312)，進而註冊由識別碼提供者指派至主要者之名字識別符。服務提供者視情況終止在服務提供者處建立之使用者/用戶端會話(步驟314)。

在處理暫存器名字識別符請求訊息之後，在服務提供者處之暫存器名字識別符服務藉由將HTTP重定向訊息(具有狀態/原因碼"302"之HTTP回應訊息)發送至用戶端而回應(步驟316)。重定向訊息使用由識別碼提供者先前提供至服務提供者之返回URI將用戶端重定向至識別碼提供者。返

回URI在重定向訊息之"位置"HTTP標頭中指明。重定向訊息之"位置"HTTP標頭亦包括一查詢組件，其例如附加至URI且在該URI內用一"?"字元區分，其含有"<lib: RegisterNameIdentifierResponse>"協定訊息。

回應於自服務提供者接收重定向訊息，用戶端如由來自服務提供者之HTTP重定向訊息中之URI指示而將HTTP Get訊息發送至識別碼提供者(步驟318)，進而結束該過程。因為在自用戶端至識別碼提供者之HTTP Get訊息中的URI仍然含有附加之"<lib: RegisterNameIdentifierResponse>"訊息，所以用戶端初始化識別碼提供者處之暫存器名字識別符操作之完成。可在識別碼提供者接收暫存器名字識別符回應訊息之後完成在圖3A中並未展示之額外處理步驟。

步驟310可包含若干不同替代性實施例用於驗證：(1)服務提供者對使用者之直接驗證；(2)在將暫存器名字識別符請求自識別碼提供者發送至服務提供者之前完成初步單一登入操作；(3)由服務提供者觸發之單一登入操作，意即為完成而自服務提供者返回發送至識別碼提供者，因此實施一挽式單一登入操作；或(4)基於在自識別碼提供者至服務提供者之暫存器名字識別符請求內的單一登入資訊之包括的單一登入操作，因此實施一推式單一登入操作。在圖3B至3E中說明此等替代者。

現參看圖3B，一資料流程圖描述一增強的基於HTTP重定向之暫存器名字識別符(RNI)設定檔，其包括一由識別碼提供者根據本發明之一實施例初始化的直接驗證步驟。

以類似於圖3A中展示之方式，圖3B描述一過程，識別碼提供者可藉由該過程改變(意即註冊)已由識別碼提供者指派至選定之服務提供者處之主要者的名字識別符；類似元素由類似參考數字識別。然而，鑒於圖3A描述一普遍驗證步驟310，圖3B中展示之過程與圖3A中展示之過程的不同之處在於包括用戶端、使用者或使用者代理與服務提供者之間之直接驗證操作(步驟320)。

現參看圖3C，一資料流程圖描述一增強的基於HTTP重定向之暫存器名字識別符(RNI)設定檔，其包括一由識別碼提供者根據本發明之一實施例初始化之用於驗證的初步單一登入操作。以類似於圖3A中所示之方式，圖3C描述一過程，識別碼提供者可藉由該過程改變(意即註冊)一由識別碼提供者指派至在選定之服務提供者處之主要者的名字識別符；類似元素由類似參考數字識別。然而，如下文中論述，鑒於圖3A描述一普遍驗證步驟310，圖3C中所示之過程與圖3A中所示之過程的不同之處在於包括一特殊驗證操作。

本發明並不在服務提供者與使用者/用戶端之間防止一直接驗證操作，藉此服務提供者直接提示一用於驗證憑證之使用者/用戶端，諸如圖3B中所說明之操作。然而，圖3A中之步驟310由一單一登入操作自識別碼提供者較佳地實施至服務提供者，使得步驟310並不要求使用者相互作用；圖3C描述一使用一單一登入操作之實施例，且圖3D至3E描述使用一單一登入操作之其它實施例。

參看圖3C，在識別碼提供者已判定用使用者之一特定服務提供者初始化暫存器名字識別符設定檔之後，識別碼提供者首先與服務提供者執行一單一登入操作。識別碼提供者將HTTP重定向訊息(具有狀態/原因碼"302"之HTTP回應訊息)發送至用戶端，亦已知為一使用者代理(諸如一網路瀏覽器應用)(步驟330)。回應於自識別碼提供者接收重定向訊息，用戶端如自識別碼提供者之HTTP重定向訊息中之URI指示而將HTTP Get訊息發送至服務提供者(步驟332)。服務提供者例如藉由驗證來自識別碼提供者之驗證符記而處理單一登入請求(步驟334)。假定成功地完成單一登入操作，接著服務提供者藉由將一HTTP重定向訊息(具有狀態/原因碼"302"之HTTP回應訊息)發送至用戶端而回應(步驟336)。重定向訊息使用由識別碼提供者先前提供至服務提供者之返回URI而將用戶端重定向至識別碼提供者；返回URI在重定向訊息之"位置"HTTP標頭中指明。回應於自服務提供者接收重定向訊息，用戶端如在來自服務提供者之HTTP重定向訊息中之URI指示而將一HTTP Get訊息發送至識別碼提供者(步驟338)，進而結束驗證/單一登入操作。

在圖3C中所示之實施例中，當其後自識別碼提供者經由用戶端將RNI請求發送至服務提供者時，服務提供者將具有用於使用者之有效會話(歸因於先前的單一登入操作)，且服務提供者並不需要以圖3A中所示之方式與使用者執行驗證操作。

本發明容納一推式單一登入操作(其在圖3D中展示)及一挽式單一登入操作(其在圖3E中展示)。使用推式單一登入操作，識別碼提供者使用發送至服務提供者之暫存器名字識別符請求嵌入某形式之驗證符記；此允許該服務提供者基於包括暫存器名字識別符請求之資訊來建構用於使用者之會話(若無會話已存在)。使用挽式單一登入操作，服務提供者中斷暫存器名字識別符處理以初始化一單一登入請求至識別碼提供者。一旦完成挽式單一登入操作，服務提供者即能夠重新開始暫存器名字識別符請求之處理。

現參看圖3D，一資料流程圖描述一增強的基於HTTP重定向之暫存器名字識別符(RNI)設定檔，其包括一由識別碼提供者根據本發明之一實施例初始化的用於驗證之推式單一登入操作。以類似於圖3A中所示之方式，圖3D描述一過程，識別碼提供者可藉由該過程而改變(意即註冊)一由該識別碼提供者指派至選定之服務提供者處之主要者的名字識別符；類似元素由類似參考數字識別。然而，如下文論述，鑒於圖3A描述一普遍驗證步驟310，在圖3D中所示之過程與圖3A中所示之過程的不同之處在於包括一特殊驗證操作。

參看圖3D，圖3D中之步驟340及步驟342類似於圖3A中展示之步驟306及步驟308；然而，步驟340及步驟342與步驟306及步驟308不同，因為識別碼提供者將單一登入資訊連同HTTP重定向訊息中之RNI請求推至用戶端(步驟340)。回應於自識別碼提供者接收重定向訊息，用戶端如

來自識別碼提供者之HTTP重定向訊息中的URI指示而將一HTTP Get訊息發送至服務提供者處之暫存器名字識別符服務(步驟342)；自用戶端至服務提供者之訊息亦含有單一登入資訊。當服務提供者處理請求時，假定可驗證單一登入請求，在於步驟312中處理RNI請求之前服務提供者基於單一登入資訊建立一用於使用者之會話(步驟344)。

現參看圖3E，一資料流程圖描述一增強的基於HTTP重定向之暫存器名字識別符(RNI)設定檔，其包括一由識別碼提供者根據本發明之一實施例初始化的用於驗證之挽式單一登入操作。以類似於圖3A中所示之方式，圖3E描述一過程，識別碼提供者可藉由該過程而改變(意即註冊)一已由識別碼提供者指派至選定之服務提供者處之主要者的名字識別符；類似元素由類似參考數字識別。然而，如下文論述，鑒於圖3A描述一普遍驗證步驟310，圖3E中展示之過程與圖3A中展示之過程的不同之處在於包括一特殊驗證操作。

參看圖3E，在服務提供者於步驟308中接收來自一特定識別碼提供者之使用者之暫存器名字識別符設定檔的請求之後，服務提供者中止處理RNI請求以與識別碼提供者執行一挽式單一登入操作。服務提供者將一HTTP重定向訊息(具有狀態/原因碼"302"之HTTP回應訊息)發送至用戶端(步驟350)。回應於自服務提供者接收重定向訊息，用戶端如由來自服務提供者之HTTP重定向訊息中的URI指示而將一HTTP Get訊息發送至識別碼提供者(步驟352)。

識別碼提供者處理請求以例如藉由產生一用於服務提供者之驗證符記而獲取單一登入資訊(步驟354)。識別碼提供者藉由將一HTTP重定向訊息(具有狀態/原因碼"302"之HTTP回應訊息)發送至該用戶端而回應(步驟356)，其中重定向訊息含有已請求之單一登入資訊。重定向訊息使用由服務提供者先前提供至識別碼提供者之返回URI而將用戶端重定向至服務提供者；返回URI在重定向訊息之"位置"HTTP標頭中指明。回應於自服務提供者接收重定向訊息，用戶端如由來自識別碼提供者之HTTP重定向訊息中之URI指示而將一HTTP Get訊息發送至服務提供者(步驟358)。當服務提供者處理請求時，假定可驗證單一登入資訊，在於步驟312中重新開始處理RNI請求之前，服務提供者基於單一登入資訊建立一用於使用者之會話(步驟359)。以此方式，服務提供者中斷暫存器名字識別符處理以初始化一挽式單一登入請求至識別碼提供者。一旦完成挽式單一登入操作，服務提供者即能夠重新開始處理暫存器名字識別符請求。

現參看圖3F，一資料流程圖描述一增強的基於HTTP重定向之暫存器名字識別符設定檔，其一由服務提供者根據本發明之一實施例初始化的普遍驗證步驟。以類似於圖2B中所示之方式，圖3F描述一過程，服務提供者可藉由該過程而設定或改變(意即註冊)由服務提供者提供至一主要者的名字識別符，已知為"<lib: SPProvidedNameIdentifier>"，其可因為多種特殊實施原因而發生。然而，如下文論述，

圖3F中展示之過程與圖2B中展示之過程的不同之處在於包括一額外驗證步驟。

用於此資料流之先決條件係使用者已鏈接識別碼提供者及服務提供者處之使用者帳戶(步驟362)且使用者已對於服務提供者而受到驗證(步驟364)。使用步驟362，要求僅係至少一"<lib: IdPProvidedNameIdentifier>"已受到設定。本發明不要求在處理中之此點處存在"<lib: SPProvidedNameIdentifier>"。使用步驟364，要求僅係使用者在某先前時間點已對於服務提供者而受到驗證且當前具有與服務提供者之有效會話。本發明並未要求會話建立之原因。舉例而言，本發明並未要求因為除執行暫存器名字識別符設定檔以外之某目的而建立此會話，亦未要求為執行暫存器名字識別符設定檔之目的而明確地建立會話。另外，本發明並未要求服務提供者處建立會話之方式；舉例而言，基於來自相應識別碼提供者之單一登入操作建立此會話或經由服務提供者之直接驗證操作建立會話既非要求亦非限制。

藉由將HTTP重定向訊息(具有狀態/原因碼"302"之HTTP回應訊息)發送至用戶端而在服務提供者處開始增強的基於HTTP重定向之暫存器名字識別符設定檔(步驟366)。重定向訊息將用戶端重定向至在識別碼提供者處之暫存器名字識別符服務之適當位置，該位置例如藉由在重定向訊息之"位置"標頭內的URI來識別。重定向訊息之"位置"HTTP標頭亦包括一查詢組件，其例如附加至URI且在URI內用

一"?"字元區分，其含有"<lib: RegisterNameIdentifierRequest>"協定訊息。

回應於自服務提供者接收重定向訊息，用戶端如由來自服務提供者之HTTP重定向訊息中的URI指示而將一HTTP Get訊息發送至識別碼提供者處之暫存器名字識別符服務(步驟368)。因為HTTP Get訊息中的URI仍然含有附加之"<lib: RegisterNameIdentifierRequest>"訊息，所以用戶端以此方式存取識別碼提供者處之暫存器名字識別符服務。

與圖2B中展示之過程相比，若識別碼提供者並不具有與使用者之有效會話，則識別碼提供者與使用者、用戶端或使用者代理執行一驗證操作(步驟370)；可假定已要求使用者/用戶端與服務提供者完成一驗證操作。識別碼提供者可由於多種原因而不具有用於使用者之有效會話：(1)可已終止先前會話；使用者可已執行一直接與服務提供者之驗證操作而無與識別碼提供者之任何先前相互作用；或(3)使用者已經由一不同識別碼提供者執行一對服務提供者之單一登入操作；或者由於某其它原因。若在步驟370中並未成功地完成驗證操作，則識別碼提供者可立即將一失敗回應返回至服務提供者，進而結束該過程。

在步驟370中，要求使用者/用戶端完成一額外驗證操作(意即除服務提供者已要求之任一驗證操作以外)，使得識別碼提供者可保證接收之暫存器名字識別符請求係連接的或可信的；另外，識別碼提供者不可保證接收之暫存器名字識別符請求訊息並非源自一惡意使用者/系統，且識別

碼提供者不可保證用戶端正執行相關聯之端使用者之RNI請求。一般而言，允許任一隨機使用者載運任一其它隨機使用者之一RNI請求並非較佳實踐。使用本發明，識別碼提供者及服務提供者處之驗證或單一登入的迫使作為暫存器名字識別符設定檔之部分而幫助保證識別碼提供者及服務提供者處之使用者至RNI請求的安全連接受到維持。

假定在步驟370中成功地完成驗證操作，識別碼提供者接著處理暫存器名字識別符請求訊息(步驟372)，進而註冊由服務提供者提供至主要者的名字識別符。識別碼提供者視情況可終止建立於識別碼提供者處之使用者/用戶端會話(步驟374)，較佳地僅當建立此會話僅用於執行暫存器名字識別符設定檔時終止建立於識別碼提供者處之使用者/用戶端會話。應注意，一般而言，識別碼提供者將不終止此會話，特別若會話在初始化暫存器名字識別符設定檔之前預先存在。

在處理暫存器名字識別符請求訊息之後，識別碼提供者處之暫存器名字識別符服務藉由將一HTTP重定向訊息(具有狀態/原因碼"302"之HTTP回應訊息)發送至用戶端而回應(步驟376)。重定向訊息使用由服務提供者先前提供至識別碼提供者之返回URI而將用戶端重定向至服務提供者。返回URI在重定向訊息之"位置"HTTP標頭中指明。重定向訊息之"位置"HTTP標頭亦包括一查詢組件，其例如附加至URI且在該URI內用一"?"字元區分，其含有"<lib:RegisterNameIdentifierResponse>"協定訊息。

回應於自識別碼提供者接收重定向訊息，用戶端如由來自識別碼提供者之HTTP重定向訊息中的URI指示而將一HTTP Get訊息發送至服務提供者(步驟378)，進而結束該過程。因為在自用戶端至服務提供者之HTTP Get訊息中的URI仍然含有附加之"<lib: RegisterNameIdentifierResponse >"訊息，所以用戶端初始化服務提供者處之暫存器名字識別符操作的完成。可在服務提供者接收暫存器名字識別符回應訊息之後完成未在圖3F中展示之額外處理步驟。

用於聯合之增強的暫存器名字識別符設定檔

如上相對於圖2A及圖2B論述，暫存器名字識別符設定檔係服務提供者可藉由其請求註冊用於一主要者之名字識別符或者識別碼提供者或服務提供者可藉由其根據先前技術自由聯盟規格改變用於一主要者之名字識別符的彼等設定檔。如上提及，如在先前技術自由聯盟規格中描述，暫存器名字識別符設定檔不允許識別碼提供者觸發名字識別符之初始設定；換言之，暫存器名字識別符設定檔不可用於鏈接先前未鏈接之帳戶，亦已知為對聯合帳戶之操作。此等設定檔僅可在預先存在之帳戶鏈接方案(意即一聯合方案)內調用。初始帳戶連接過程僅可由服務提供者在特定單一登入設定檔之範疇內調用，其經常稱為一聯合設定檔。

本發明藉由允許識別碼提供者為建立初始帳戶連接之目的而觸發暫存器名字識別符設定檔來解決此不足。如下文中相對於圖4A及圖4B更詳細地說明，此方法要求使用者

(大概係為其執行暫存器名字識別符設定檔的主要者)在初始暫存器名字識別符操作期間對識別碼提供者及服務提供者進行明確驗證。雖然在圖4A及圖4B內說明之例示性實施例使用基於HTTP之通信，但是本發明並不限於基於HTTP之通信，且可使用其它通信協定。

現參看圖4A，一資料流程圖描述一由識別碼提供者初始化之增強的基於HTTP重定向之暫存器名字識別符設定檔以執行帳戶連接操作，其根據本發明之一實施例可視情況由一單一登入操作跟隨。以類似於圖3A中所示之方式，圖4A描述一過程，識別碼提供者可藉由該過程註冊用於一主要者的新名字識別符，其中在該主要者之具有一給定服務提供者之識別碼提供者處當前不存在名字識別符；在先前技術自由聯盟規格中並未指明此功能性。另外，圖4A描述說明一實例之額外處理步驟，在該實例中本發明之增強的基於HTTP重定向之暫存器名字識別符設定檔併入一組交易中，其中在識別碼提供者處之使用者帳戶與服務提供者處之使用者帳戶經鏈接在一起。在已執行帳戶鏈接操作之後，識別碼提供者可初始化與依賴於鏈接之帳戶的服務提供者之單一登入操作。

過程開始於用戶端發送用於識別碼提供者處之受保護或受控資源之HTTP請求訊息(步驟402)，諸如一登入網頁。識別碼提供者隨後要求用戶端完成一驗證操作(步驟404)，其後識別碼提供者將一回應返回至用戶端(步驟406)。在此實例中，識別碼提供者返回聯合替代者之提供；此等聯合

替代者可為與在相同聯合內之識別碼提供者相互作用的一列服務提供者。

舉例而言，識別碼提供者可返回一含有在聯合計算環境內與識別碼提供者相互作用之一列第三方入口的網頁；返回之網頁表示允許使用者自該列第三方入口選擇一第三方入口的形式。用戶端使用者(一在聯合內之主要者)可或可不具有在第三方入口中之一者處之先前建立之使用者帳戶；然而，假定使用者已在第三方入口中之一者處建立一使用者帳戶，返回之網頁係一允許使用者將第三方入口處之使用者帳戶與識別碼提供者處之使用者帳戶鏈接的形式。換言之，由用戶端自識別碼提供者接收之網頁允許使用者初始化一帳戶鏈接操作以使得第三方入口隨後相對於使用者鏈接至識別碼提供者。用戶端使用者可例如藉由在網頁中選擇一格式化為一形式且在網路瀏覽器之視窗內提出至使用者的多選鈕(check box)而選擇一第三方入口，其中多選鈕與一表示由服務提供者操作之域的特定第三方入口相關聯。在選擇特定控制(諸如"OK"按鈕或"提交"按鈕)後，來自該形式之適當內容即自用戶端發送至識別碼提供者(例如在HTTP Post訊息內)，進而指示使用者需要將識別碼提供者處之使用者帳戶與選定之服務提供者相聯合(步驟408)。

在自用戶端接收請求以初始化聯合操作之後，識別碼提供者建置一暫存器名字識別符請求訊息(步驟410)。本發明之增強的基於HTTP重定向之暫存器名字識別符設定檔接

著藉由將一HTTP重定向訊息(具有狀態/原因碼"302"之HTTP回應訊息)發送至用戶端而開始於識別碼提供者處(步驟412)。重定向訊息將用戶端重定向至服務提供者處之暫存器名字識別符服務之適當位置，該位置例如由在重定向訊息之"位置"標頭內的URI識別。重定向訊息之"位置"HTTP標頭亦包括一查詢組件，其例如附加至URI且在該URI內用一"?"字元區分，其含有在步驟410中先前建置之"<lib: RegisterNameIdentifierRequest>"協定訊息。

回應於自識別碼提供者接收重定向訊息，用戶端如由來自該識別碼提供者之HTTP重定向訊息中的URI指示而將一HTTP Get訊息發送至服務提供者處之暫存器名字識別符服務(步驟414)。若使用者並非已具有與服務提供者之有效會話，則服務提供者收集使用者之驗證憑證(例如，使用者名字及通行碼)且驗證此等憑證(步驟416)，進而要求一額外使用者相互作用(意即除識別碼提供者可要求之任何相互作用以外)。要求此相互作用以使得服務提供者可判定使用者(為其請求聯合/暫存器名字識別符)之本端識別碼。並不要求服務提供者回應於此驗證請求而建立一用於使用者之會話；服務提供者可僅驗證提出之憑證以判定使用者之識別碼及可靠性。因此，並不要求服務提供者管理使用者之會話，以如在單一HTTP請求/回應對之範疇內完成服務提供者側功能性而完成此暫存器名字識別符設定檔。

應注意，在某些情況下，使用者將已在服務提供者處建立一帳戶。然而，若使用者在服務提供者處並不具有一預

先存在的帳戶，則服務提供者可選擇回應於此驗證/RNI請求而建立一用於使用者之帳戶；一旦此帳戶經建立，RNI處理之剩餘物將如圖4A中所示而進行，意即將服務提供者處之使用者帳戶與識別碼提供者處之使用者帳戶相聯合。

步驟416之部分亦可包括服務提供者與使用者之相互作用藉此服務提供者可選擇例如藉由提供一含有一訊息之特殊格式化的網頁來通知請求之使用者聯合，該訊息諸如：

試圖與吾人之識別碼提供者"X"聯合/鏈接帳戶。藉由將登入資訊提供給吾人，同意此鏈接。一旦已建立此鏈路，將能夠執行自識別碼提供者"X"至本端帳戶之單一登入操作。若不希望完成此行為，則選擇"CANCEL"。

來自使用者之取消請求立即將一失敗回應產生至識別碼提供者。可將此頁作為來自服務提供者之登入請求之部分提出，進而向使用者解釋為何請求使用者之驗證憑證。

若由於使用者具有預先存在的與服務提供者之有效會話而並不要求一用於收集驗證憑證之明確使用者相互作用，則服務提供者可使用步驟416來尋求使用者之"同意聯合"，其係僅在先前技術自由聯盟規格之SSO-聯合設定檔內定義之行為。應注意此方案(意即其中帳戶並未鏈接；使用者已對於識別碼提供者而受到驗證且視情況可對於服務提供者而受到驗證；且使用者請求自識別碼提供者之帳戶鏈接)在用於一暫存器名字識別符設定檔之先前技術自由聯盟規格中係不可能的。

亦應注意，因為使用者之服務提供者帳戶並未與使用者

之識別碼提供者帳戶聯合，所以自識別碼提供者至服務提供者之單一登入操作係不可能的；使用者必須直接將驗證憑證/識別碼資訊提出給服務提供者。使用者可能已將服務提供者處之使用者帳戶與一不同識別碼提供者聯合，在此狀況下來自此其它識別碼提供者之單一登入操作係可能的。因此，或者，在服務提供者與請求識別碼提供者之間拒絕新聯合之某選擇可提出給使用者，例如遵從服務提供者處之使用者帳戶與一不同識別碼提供者之預先存在的聯合。

若在已經由來自一不同識別碼提供者之單一登入操作建立之會話的內容中於服務提供者處接收暫存器名字識別符請求訊息，則服務提供者可選擇在進行暫存器名字識別符處理之前重新提示使用者驗證憑證。一其中需要此之方案的一實例如下：一使用者具有一服務提供者的兩個相異帳戶，一者鏈接至使用者之雇主作為其識別碼提供者且一者係使用者之個人帳戶並且並不與其雇主相鏈接。若使用者接著希望將此第二個人帳戶與一不同識別碼提供者(例如，使用者之銀行)相鏈接，則服務提供者必須注意保證自銀行接收之任一暫存器名字識別符請求訊息與使用者之個人帳戶正確鏈接。因此，若使用者試圖將其銀行與個人帳戶相聯合而其具有與來自其雇主之服務提供者的有效會話，則負擔係服務提供者保證完成適當帳戶鏈接。

若使用者試圖聯合已與不同識別碼提供者聯合之帳戶，則應例如藉由提供一含有一訊息之特殊格式化之網頁來提

示使用者，該訊息諸如：

當前與識別碼提供者"X"相聯合--現在希望與識別碼提供者"Y"相聯合嗎？

一使用者可能具有與單一服務提供者相關聯之多個識別碼提供者。雖然此並非一普通事件，但是此例如當一使用者具有一由充當其識別碼提供者的使用者之雇主發起或以某方式與使用者之雇主聯繫的與服務提供者之帳戶時可發生；使用者甚至未意識到服務提供者資源並非由識別碼提供者提供。使用者亦可具有與相同服務提供者之個人帳戶；舉例而言，除經由使用者之個人帳戶的個人銷售服務以外，一服務提供者可經由使用者之雇主提供股票選擇管理。

假定在步驟416中成功完成驗證/識別操作，服務提供者接著處理暫存器名字識別符請求訊息(步驟418)，進而註冊由識別碼提供者指派至主要者的名字識別符且鏈接主要者之識別碼以使得經由由識別碼提供者保持之資訊將使用者之帳戶鏈接在一起。服務提供者視情況可終止可在服務提供者處建立之任一使用者/用戶端會話(步驟420)。

在處理暫存器名字識別符請求訊息之後，服務提供者處之暫存器名字識別符服務藉由將一HTTP重定向訊息(具有狀態/原因碼"302"之HTTP回應訊息)發送至用戶端而回應(步驟422)。此訊息可亦包括某形式之用戶端側維持資訊(諸如一HTTP cookie)，該資訊係由服務提供者設定且識別作為使用者之識別碼提供者的識別碼提供者；此將立即使

得使用者能夠執行一自識別碼提供者至服務提供者的單一登入操作。

重定向訊息使用由識別碼提供者先前提供至服務提供者之返回URI而將用戶端重定向至識別碼提供者。返回URI在重定向訊息之"位置"HTTP標頭中指明。重定向訊息之"位置"HTTP標頭亦包括一查詢組件，其例如附加至URI且在該URI內用一"?"字元區分，其含有"<lib：RegisterNameIdentifierResponse>"協定訊息。

回應於自服務提供者接收重定向訊息，用戶端如由來自服務提供者之HTTP重定向訊息中的URI指示而將一HTTP Get訊息發送至識別碼提供者(步驟424)。因為在自用戶端至識別碼提供者之HTTP Get訊息中的URI仍然含有附加之"<lib： RegisterNameIdentifierResponse>"訊息，所以用戶端初始化在識別碼提供者處之暫存器名字識別符操作之完成。識別碼提供者處理來自經由用戶端重定向之服務提供者的暫存器名字識別符回應訊息(步驟426)。

假定來自服務提供者之回應指示一成功暫存器名字識別符操作，識別碼提供者將一回應發送至用戶端用於起初在步驟408中請求之聯合操作(步驟428)；此回應可含有帳戶鏈接操作以及至服務提供者處之聯合資源之鏈路的成功完成的指示，例如以嵌入在返回至在用戶端上執行之網路瀏覽器之網頁內的超鏈接之形式。

使用者接著可在用戶端處操作網路瀏覽器以選擇或存取如在自識別碼提供者接收之網頁內提供的服務提供者處之

受控或受保護資源，且用戶端將一HTTP請求訊息發送至服務提供者用於請求之資源(步驟430)。假定識別碼提供者處之使用者帳戶與服務提供者現鏈接在一起，服務提供者可與用戶端及/或識別碼提供者相互作用以執行一驗證操作(步驟432)；舉例而言，識別碼提供者可提供一如由服務提供者通過HTTP重定向訊息經由用戶端請求的驗證符記。假定驗證操作係成功的，服務提供者將一HTTP回應訊息發送至用戶端(步驟434)。自服務提供者至用戶端之回應可為一表示第三方入口服務之網頁，該等第三方入口服務基於使用者之識別碼而對於使用者係尤其可用的；換言之，網頁較佳含有經特製而用於使用者之資訊內容。另外，網頁可以聯合方式包括至識別碼提供者處之受保護或受控資源的鏈路。

如以上提及，步驟420係可選的但較佳地包括在本發明之暫存器名字識別符設定檔內應建立一會話；若在步驟420中建立且並未終止用於暫存器名字識別符之操作的會話，則在步驟430中由於下列原因而可由服務提供者產生未定義之結果。在於步驟430中之自用戶端至服務提供者之隨後請求期間，服務提供者可認為請求源自相同用戶端，例如歸因於一伴隨來自用戶端之請求的HTTP cookie，其中HTTP cookie含有一會話識別符，其中此會話如對於服務提供者直接受到驗證而經結合至使用者。若先前會話並未終止，則服務提供者可認為在HTTP cookie內之會話識別符係有效會話識別符，進而使得服務提供者使

用與先前建構之會話相關聯之資訊來回應用戶端；然而，此資訊係陳舊的。若先前建立之會話包括一使用者帳戶資訊子集之複本，則服務提供者基於來自使用者帳戶之資訊之此子集而返回一回應，而在先前建立之會話經建置之後，服務提供者處之使用者帳戶變得與識別碼提供者處之使用者帳戶聯合。因此，服務提供者應使用在服務提供者執行使用者之暫存器名字識別符操作之後建立的服務提供者處之使用者帳戶中的資訊來回應來自用戶端之隨後請求，以使得使用者接收可具有聯合資訊之回應；一保證使用最近使用者帳戶資訊之方式係保證在步驟420中終止先前會話，或在步驟420中從未建立會話。

舉例而言，服務提供者可提供一電子貿易域內之某些服務的購買刺激，該電子貿易域用於具有與識別碼提供者聯合之帳戶的使用者。若服務提供者將使用陳舊的使用者帳戶資訊，則使用者並不接收該刺激直至服務提供者處之使用者的下一會話(意即使用者對於由服務提供者操作之電子貿易域的隨後訪問)。然而，在使用者之帳戶已鏈接在一起之後，刺激即對於使用者可用。藉由終止較早會話，此方案受到避免。

現參看圖4B，一資料流程圖根據本發明之一實施例描述一由服務提供者為執行一帳戶鏈接操作而初始化之增強的基於HTTP重定向之暫存器名字識別符設定檔，該帳戶鏈接操作視情況可由一單一登入操作跟隨。以類似於圖3B中所示之方式，圖4B描述一過程，服務提供者藉由該過程可

註冊一用於一主要者的新名字識別符，其中在該主要者之具有一給定服務提供者之識別碼提供者處當前不存在名字識別符；在先前技術自由聯盟規格中並未指明此功能性。另外，圖4A描述說明一實例之額外處理步驟，其中本發明之增強的基於HTTP重定向之暫存器名字識別符設定檔併入其中在識別碼提供者處之使用者帳戶與服務提供者處之使用者帳戶鏈接在一起的一組交易中。在執行帳戶鏈接操作之後，識別碼提供者可初始化與依賴於鏈接之帳戶之服務提供者的單一登入操作。

過程開始於用戶端發送一用於服務提供者處之受保護或受控資源的HTTP請求訊息(步驟452)，諸如一登入網頁。服務提供者隨後要求用戶端完成一驗證操作(步驟454)，其後服務提供者將一回應返回至用戶端(步驟456)。在此實例中，服務提供者返回聯合替代者之一提供；此等聯合替代者可為與服務提供者在相同聯合內相互作用的一列識別碼提供者。

舉例而言，服務提供者可返回一含有在聯合計算環境內與服務提供者相互作用之一列第三方入口的網頁；返回之網頁表示一允許使用者自該列第三方入口選擇一第三方入口的形式。用戶端之使用者(其係聯合內之一主要者)可或可不具有在第三方入口中之一者處先前建立之使用者帳戶；然而，假定使用者已在第三方入口中之一者處建立一使用者帳戶，返回之網頁係一允許使用者將第三方入口處之使用者帳戶與識別碼提供者處之使用者帳戶相鏈接的形

式。換言之，由用戶端自服務提供者接收之網頁允許使用者初始化一帳戶鏈接操作以使得第三方入口相對於使用者隨後經鏈接至服務提供者。用戶端使用者可例如藉由在網頁中選擇一格式化為一形式且在網路瀏覽器之視窗內提出至使用者的多選鈕而選擇一第三方入口，其中多選鈕與一表示由識別碼提供者操作之域的特定第三方入口相關聯。在選擇特定控制(諸如"OK"按鈕或"提交"按鈕)後，來自該形式之適當內容即自用戶端發送至服務提供者(例如在HTTP Post訊息內)，進而指示使用者需要將服務提供者處之使用者帳戶與選定之識別碼提供者相聯合(步驟458)。

在自用戶端接收請求以初始化聯合操作之後，服務提供者建置一暫存器名字識別符請求訊息(步驟460)。本發明之增強的基於HTTP重定向之暫存器名字識別符設定檔接著藉由將一HTTP重定向訊息(具有狀態/原因碼"302"之HTTP回應訊息)發送至用戶端而開始於服務提供者處(步驟462)。重定向訊息將用戶端重定向至識別碼提供者處之暫存器名字識別符服務之適當位置，該位置例如由在重定向訊息之"位置"標頭內的URI識別。重定向訊息之"位置"HTTP標頭亦包括一查詢組件，其例如附加至URI且在該URI內用一"?"字元區分，其含有在步驟460中先前建置之"<lib: RegisterNameIdentifierRequest>"協定訊息。

回應於自服務提供者接收重定向訊息，用戶端如由來自該服務提供者之HTTP重定向訊息中的URI指示而將一HTTP Get訊息發送至識別碼提供者處之暫存器名字識別符

服務(步驟464)。若使用者並非已具有與識別碼提供者之有效會話，則識別碼提供者收集使用者之驗證憑證(例如，使用者名字及通行碼)且驗證此等憑證(步驟466)，進而要求一額外使用者相互作用(意即除服務提供者可要求之任何相互作用以外)。要求此相互作用以使得識別碼提供者可判定使用者(為其請求聯合/暫存器名字識別符)之本端識別碼。並不要求識別碼提供者回應於此驗證請求而建立一用於使用者之會話；然而，因為一回應將發送至服務提供者而由服務提供者用於單一登入目的，所以識別碼提供者應建立一用於使用者之會話。

應注意，在某些情況下，使用者將已在識別碼提供者處建立一帳戶。然而，若使用者在識別碼提供者處並不具有一預先存在的帳戶，則識別碼提供者可選擇回應於此驗證/RNI請求而建立一用於使用者之帳戶；一旦此帳戶經建立，RNI處理之剩餘物將如圖4B中所示而進行，意即將識別碼提供者處之使用者帳戶與服務提供者處之使用者帳戶相聯合。

步驟466之部分亦可包括識別碼提供者與使用者之相互作用藉此識別碼提供者可選擇例如藉由提供一含有一訊息之特殊格式化的網頁來通知請求之使用者聯合，該訊息諸如：

試圖與吾人之服務提供者"X"聯合/鏈接帳戶。藉由將登入資訊提供給吾人，同意此鏈接。一旦已建立此鏈路，將能夠執行自服務提供者"X"至本端帳戶之單一登入操作。

若不希望完成此行為，則選擇"CANCEL"。

來自使用者之取消請求立即將一失敗回應產生至服務提供者。可將此頁作為來自識別碼提供者之登入請求之部分提出，進而向使用者解釋為何請求使用者之驗證憑證。

若由於使用者具有預先存在的與識別碼提供者之有效會話而並不要求一用於收集驗證憑證之明確使用者相互作用，則識別碼提供者可使用步驟466來尋求使用者之"同意聯合"。應注意此方案(意即其中帳戶並未鏈接；使用者已對於服務提供者而受到驗證且視情況可對於識別碼提供者而受到驗證；且使用者請求自識別碼提供者之帳戶鏈接)在用於一暫存器名字識別符設定檔之先前技術自由聯盟規格中係不可能的。

應注意使用者可能已將識別碼提供者處之使用者帳戶與其它服務提供者相聯合；然而，此不應影響使用者之將(另一)服務提供者帳戶與此識別碼提供者相聯合之請求。在此狀況下，需要向使用者提出拒絕與此服務提供者聯合的某選項。

假定在步驟466中成功完成驗證/識別操作，識別碼提供者接著處理暫存器名字識別符請求訊息(步驟468)，進而註冊由服務提供者指派至主要者的名字識別符("SPProvidedNameIdentifier")。應注意，因為先前技術自由聯盟規格要求帳戶經斷開鏈接至少一"IdPProvidedNameIdentifier"，所以識別碼提供者亦將建立此名字識別符值、註冊其用於使用者且試圖將其返回至服

務提供者。此允許主要者之識別碼之鏈接以使得使用者之帳戶經由由識別碼提供者及服務提供者保持之資訊而鏈接在一起。識別碼提供者接著視情況可終止可已在識別碼提供者處建立之任一使用者/用戶端會話(步驟470)。

在處理暫存器名字識別符請求訊息之後，識別碼提供者處之暫存器名字識別符服務藉由將一HTTP重定向訊息(具有狀態/原因碼"302"之HTTP回應訊息)發送至用戶端而回應(步驟472)。此訊息亦包括識別碼提供者之名字識別符("IdPProvidedNameIdentifier")；此允許服務提供者使用"IdPProvidedNameIdentifier"資料值與識別碼提供者關於使用者而交談。

重定向訊息使用由服務提供者先前提供至識別碼提供者之返回URI而將用戶端重定向至服務提供者。返回URI在重定向訊息之"位置"HTTP標頭中指明。重定向訊息之"位置"HTTP標頭亦包括一查詢組件，其例如附加至URI且在該URI內用一"?"字元區分，其含有"<lib: RegisterNameIdentifierResponse>"協定訊息。

回應於自識別碼提供者接收重定向訊息，用戶端如由來自識別碼提供者之HTTP重定向訊息中的URI指示而將一HTTP Get訊息發送至服務提供者(步驟474)。因為在自用戶端至識別碼提供者之HTTP Get訊息中的URI仍然含有附加之"<lib: RegisterNameIdentifierResponse>"訊息，所以用戶端初始化在識別碼提供者處之暫存器名字識別符操作之完成。識別碼提供者處理來自經由用戶端重定向之服務

提供者的暫存器名字識別符回應訊息(步驟476)。

假定來自識別碼提供者之回應指示一成功暫存器名字識別符操作，服務提供者將一回應發送至用戶端用於起初在步驟458中請求之聯合操作(步驟478)；此回應可含有帳戶鏈接操作以及至服務提供者處之聯合資源之鏈路的成功完成的指示，例如以嵌入在返回至在用戶端上執行之網路瀏覽器之網頁內的超鏈接之形式。

使用者接著可在用戶端處操作網路瀏覽器以選擇或存取服務提供者處之受控或受保護資源(步驟480)。假定識別碼提供者處之使用者帳戶與服務提供者現鏈接在一起，識別碼提供者可與用戶端及/或服務提供者相互作用以執行一驗證操作(步驟482)；舉例而言，識別碼提供者可提供一如由服務提供者通過HTTP重定向訊息經由用戶端請求的驗證符記。假定驗證操作係成功的，服務提供者將一HTTP回應訊息發送至用戶端(步驟484)。自服務提供者至用戶端之回應可為一表示第三方入口服務之網頁，該等第三方入口服務基於使用者之識別碼而對於使用者係尤其可用的；換言之，網頁較佳含有經特製而用於使用者之資訊內容。另外，網頁可以聯合方式包括至服務提供者處之受保護或受控資源的鏈路。

如上提及，步驟470係可選的。若服務提供者隨後管理用於使用者之會話，則識別碼提供者不應終止此會話。此接著，因為服務提供者應保證此會話結合至識別碼提供者且係可控制的，諸如具有一識別碼提供者初始化之單一登

出請求。若識別碼提供者會話受到終止，則此係不可能的。

結論

鑒於如上提供之本發明之詳細描述，本發明之優點應為顯而易見的。使用在先前技術自由聯盟規格中之暫存器名字識別符設定檔，惡意使用者可充當識別碼提供者或服務提供者以相對於使用者之帳戶欺騙暫存器名字識別符操作，進而引起狀況使得惡意使用者存取使用者之帳戶。使用本發明，在暫存器名字識別符操作期間要求一額外驗證操作，進而使暫存器名字識別符設定檔更安全，以使得服務提供者或識別碼提供者可信任由識別碼提供者或服務提供者接收之單一登入事件。

此外，本發明提供一安全暫存器名字識別符設定檔，其允許使用者之安全帳戶連接在單一登入操作流之外部初始化且允許識別碼提供者或服務提供者初始化此連接。在先前技術自由聯盟規格中未描述此特徵，且在根據先前技術自由聯盟規格實施之系統中包括此特徵而並非亦要求額外操作以迫使服務提供者回應於來自識別碼提供者之使用者請求而請求聯合/單一登入操作係不可能的。

注意儘管本發明已在全功能資料處理系統之內容中受到描述但是普通熟習此項技術者應瞭解本發明之過程能夠以電腦可讀媒體中之指令之形式及多種其它形式而分散，而不考慮實際上用於進行分散之特定類型之訊號承載媒體係重要的。電腦可讀媒體之實例包括媒體如EPROM、

ROM、磁帶、紙張、軟碟、硬碟機、RAM、以及CD-ROM及傳輸類型媒體，諸如數位及類比通信鏈路。

將一種方法普遍設想為一導致一所要結果的自一致步驟序列。此等步驟要求實體量之實體操作。通常，儘管並不必要，但是電訊號或磁訊號之形式的此等量能夠受到儲存、傳送、組合、比較及另外的操作。主要因為共有使用，將此等訊號稱為位元、值、參數、項、元素、物件、符號、字元、術語、數或其類似物，其時常係方便的。然而，應注意，所有此等術語及類似術語將與適當物理量相關聯且僅係應用於此等量之方便標籤。

本發明之描述已為說明之目的而提出但並非希望係完全的或限於所揭示之實施例。普通熟習此項技術者將易瞭解諸多修正及變化。選擇實施例以解釋本發明之原則及其實際應用且使其它普通熟習此項技術者能夠理解本發明，以實施適合其它涵蓋之用途的各種實施例及各種修正。

【圖式簡單說明】

圖1A描述一資料處理系統典型網路，其中之每一者可實施本發明；

圖1B描述一可用於一可實施本發明之資料處理系統內的典型電腦架構；

圖1C描述一說明一當一用戶端試圖存取一位於伺服器處之受保護資源時可使用之典型驗證過程的資料流程圖；

圖1D描述一說明一可實施本發明之典型基於Web之環境的網路圖；

圖1E描述一說明一需要來自一使用者之多個驗證操作之典型線上交易的一實例的方塊圖；

圖2A-圖2B描述說明如在自由聯盟規格內定義之基於HTTP重定向之暫存器名字識別符設定檔的資料流程圖；

圖3A描述一資料流程圖，其說明一增強之基於HTTP重定向之暫存器名字識別符(RNI)設定檔，包括一由一識別碼提供者根據本發明之一實施例初始化的普遍驗證步驟；

圖3B描述一資料流程圖，其說明一增強之基於HTTP重定向之暫存器名字識別符(RNI)設定檔，包括一由一識別碼提供者根據本發明之一實施例初始化的直接驗證步驟；

圖3C描述一資料流程圖，其說明一增強之基於HTTP重定向之暫存器名字識別符(RNI)設定檔，包括一由一識別碼提供者根據本發明之一實施例初始化之用於驗證的初步單一登入操作；

圖3D描述一資料流程圖，其說明一增強之基於HTTP重定向之暫存器名字識別符(RNI)設定檔，包括一由一識別碼提供者根據本發明之一實施例初始化之用於驗證的推式單一登入操作；

圖3E描述一資料流程圖，其說明一增強之基於HTTP重定向之暫存器名字識別符(RNI)設定檔，包括一由一識別碼提供者根據本發明之一實施例初始化之用於驗證的挽式單一登入操作；

圖3F描述一資料流程圖，其說明一增強之基於HTTP重定向之暫存器名字識別符(RNI)設定檔，包括一由一服務

提供者根據本發明之一實施例初始化的普遍驗證步驟；

圖4A根據本發明之一實施例描述一資料流程圖，其說明一由一識別碼提供者為執行一帳戶鏈接操作而初始化的增強之基於HTTP重定向之暫存器名字識別符設定檔，該帳戶鏈接操作視情況可由一單一登入操作跟隨；及

圖4B根據本發明之一實施例描述一資料流程圖，其說明一由一服務提供者為執行一帳戶鏈接操作而初始化的增強之基於HTTP重定向之暫存器名字識別符設定檔，該帳戶鏈接操作視情況可由一單一登入操作跟隨。

【主要元件符號說明】

100	分散式資料處理系統
101	網路
102	伺服器
103	伺服器
104	儲存單元
105	用戶端
106	用戶端
107	用戶端
109	用戶端
110	網路
111	電話
112	無線鏈路
113	PDA
114	無線鏈路

115	無線鏈路
116	無線通信鏈路
120	資料處理系統
122	中央處理單元(CPU)
123	系統匯流排
124	隨機存取記憶體(RAM)
126	唯讀記憶體
128	輸入/輸出配接器
130	印表機
132	碟片單元
134	通信配接器
136	通信鏈路
140	鍵盤
142	滑鼠
144	顯示配接器
146	顯示設備.
148	使用者介面配接器
150	用戶端工作站
151	伺服器
170	瀏覽器
171	用戶端
172	web應用伺服器
173	DNS域
174	web應用伺服器

175	DNS域
176	驗證伺服器
177	驗證伺服器
190	使用者
191	ISP域
192	驗證管理器
193	政府域
194	驗證管理器
195	銀行域
196	驗證管理器
197	電子貿易域
198	驗證管理器

五、中文發明摘要：

本文提出一種方法、一種系統、一種裝置及一種電腦程式產品，其用於改良一聯合計算環境內之一暫存器名字識別符設定檔，以使得該暫存器名字識別符設定檔得到增強，以在該聯合計算環境內諸如一識別碼提供者與一服務提供者的兩個聯合實體之間更安全地連接。在第一聯合實體將一用於一主要者之暫存器名字識別符請求發送至第二聯合實體之後，該第二聯合實體執行一用於該主要者之驗證操作。回應於成功地完成該驗證操作，該第二聯合實體註冊或修正已自接收之暫存器名字識別符請求提取之一用於該主要者的名字識別符。

六、英文發明摘要：

十一、圖式：

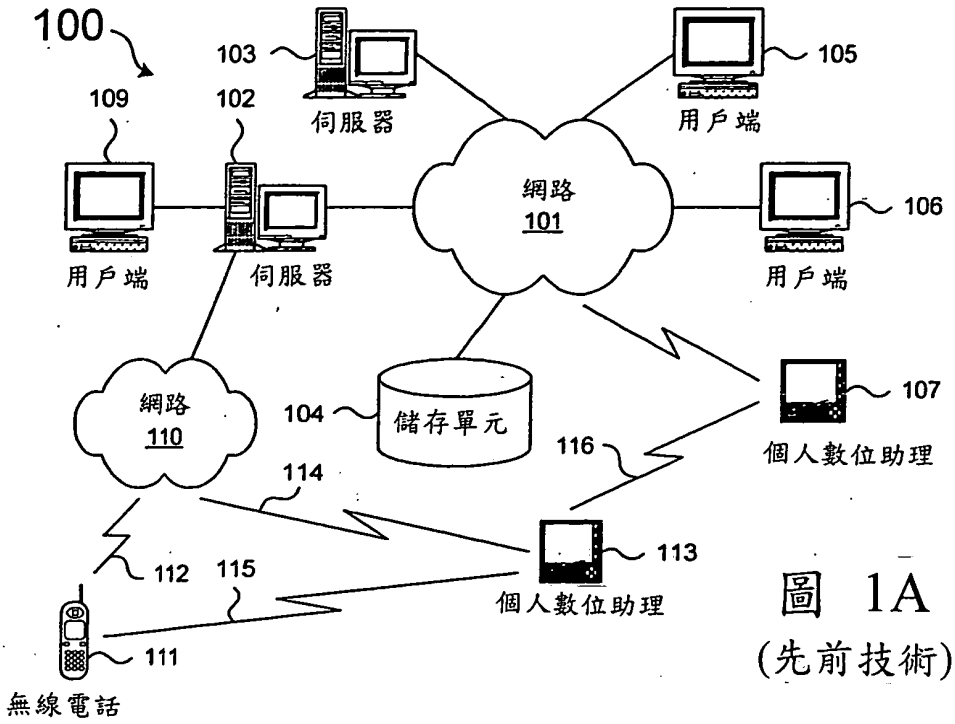


圖 1A
(先前技術)

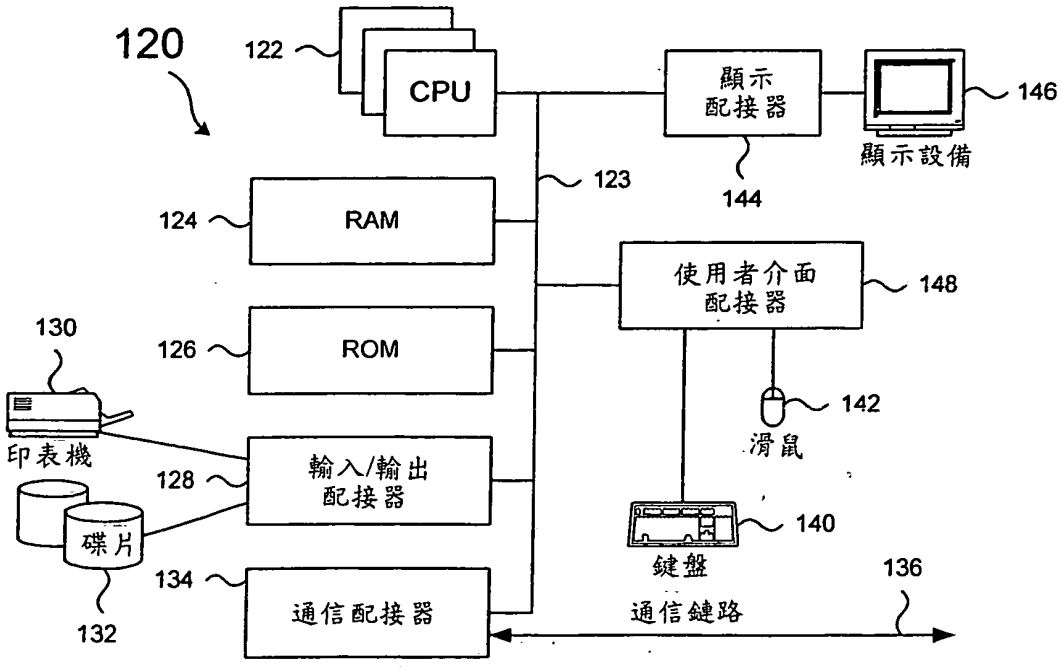


圖 1B
(先前技術)

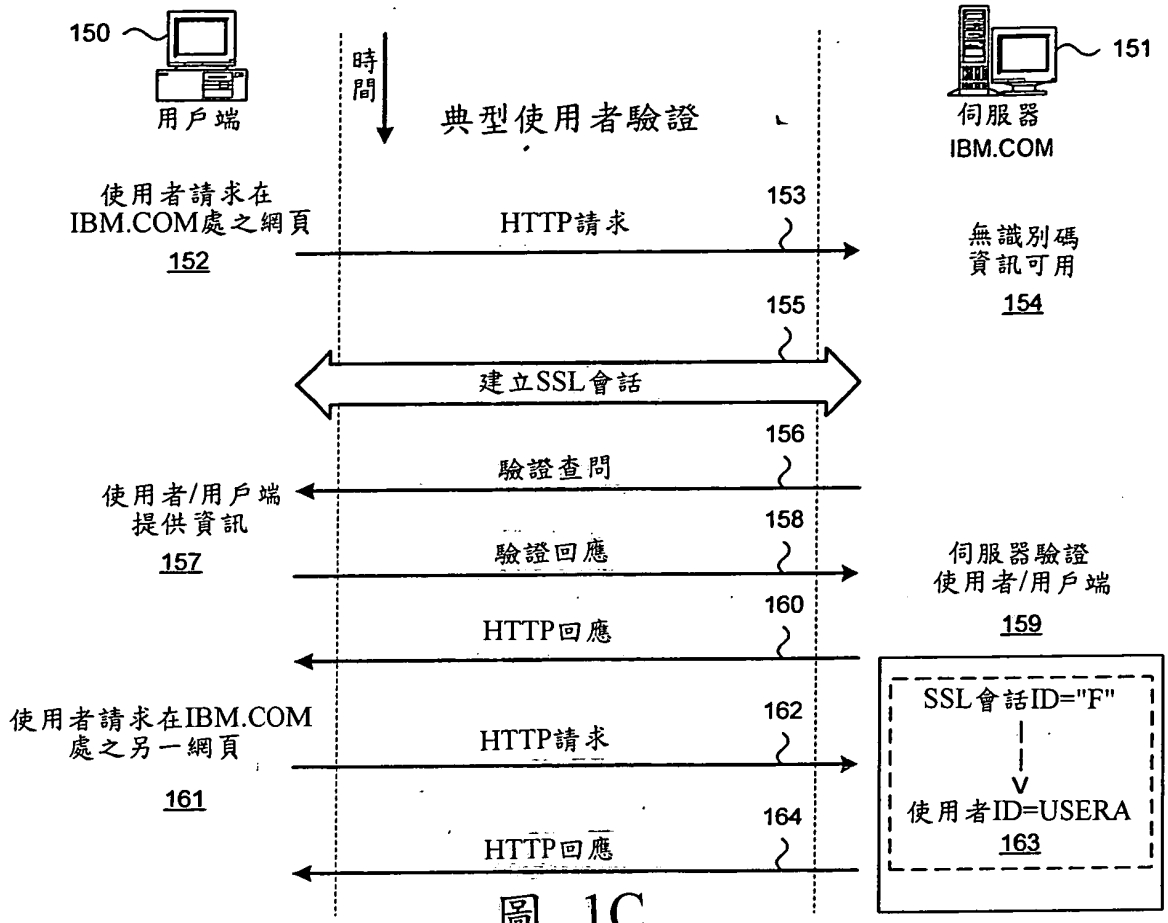


圖 1C
(先前技術)

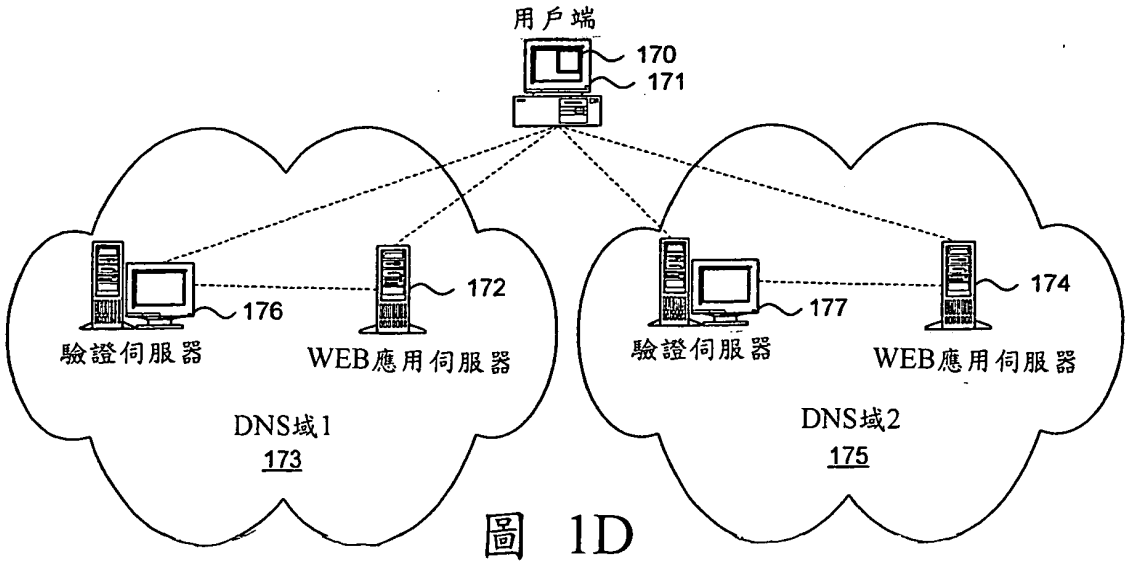


圖 1D
(先前技術)

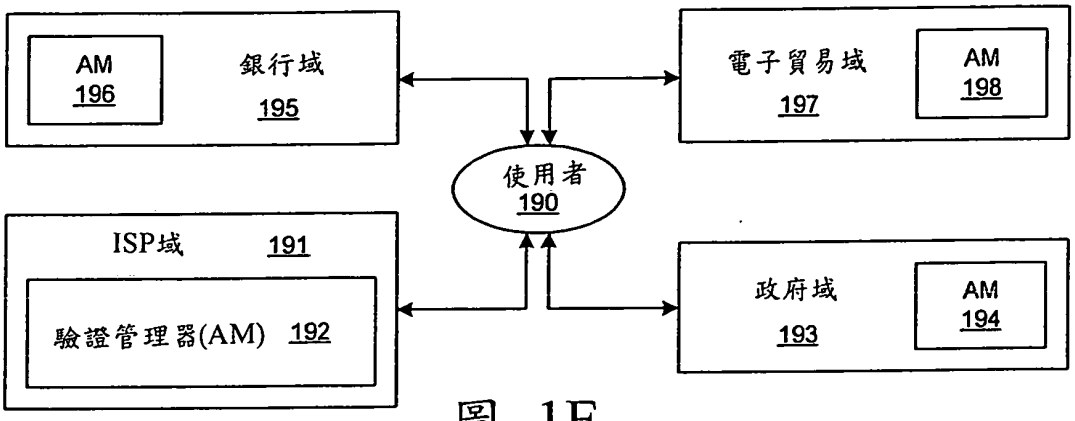


圖 1E
(先前技術)

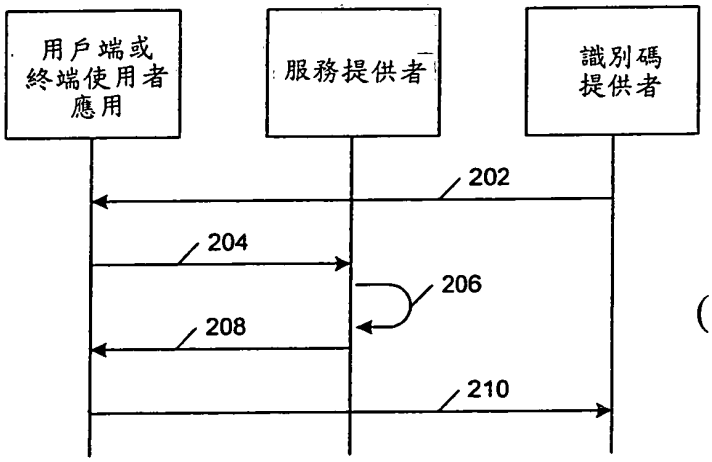


圖 2A
(先前技術)

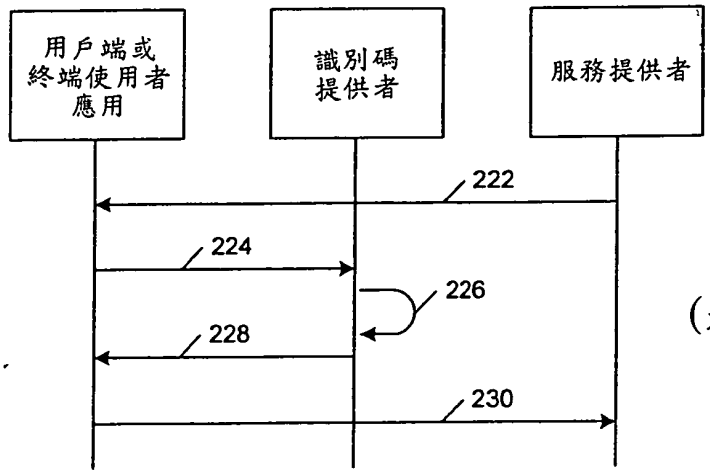
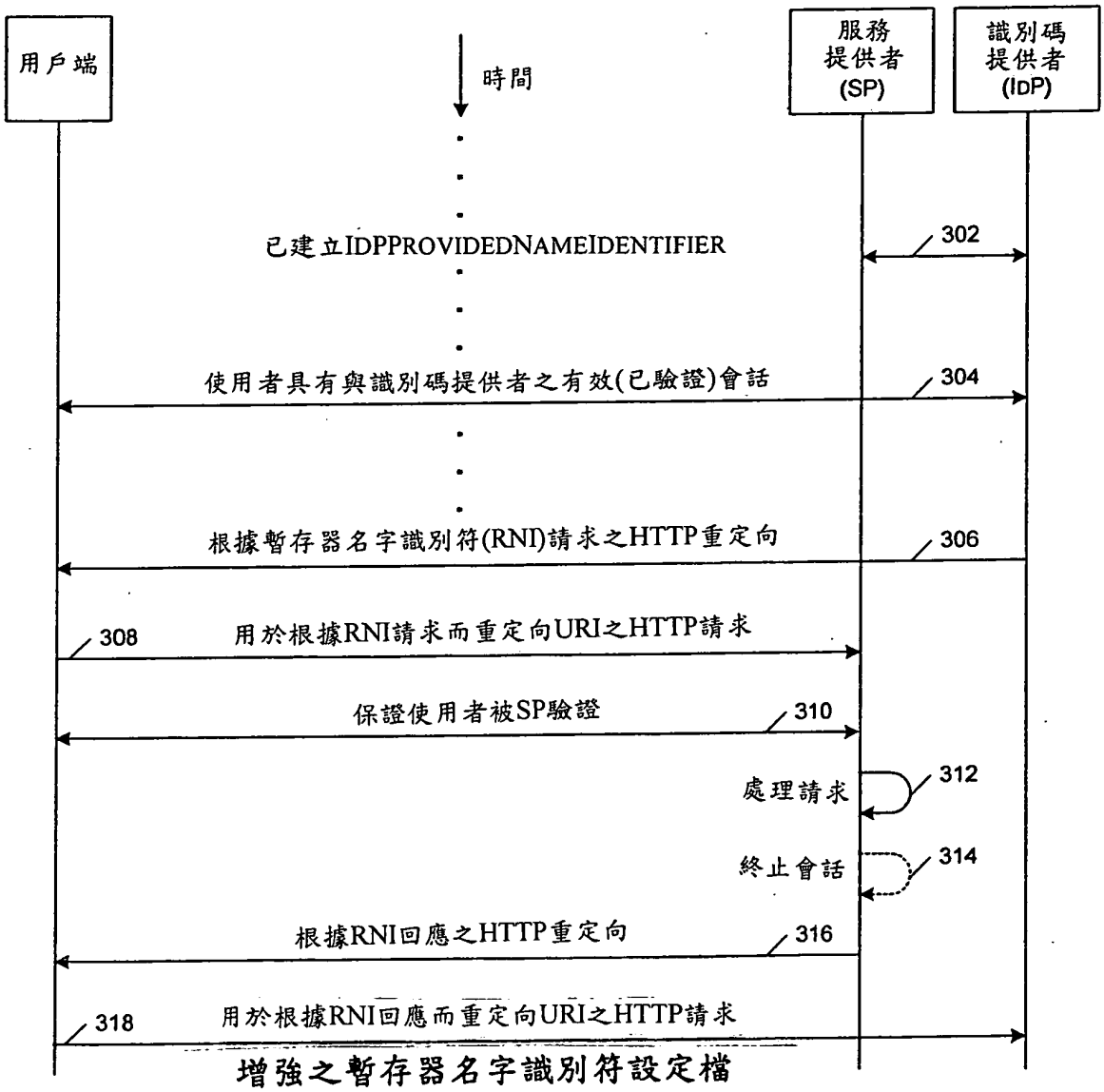
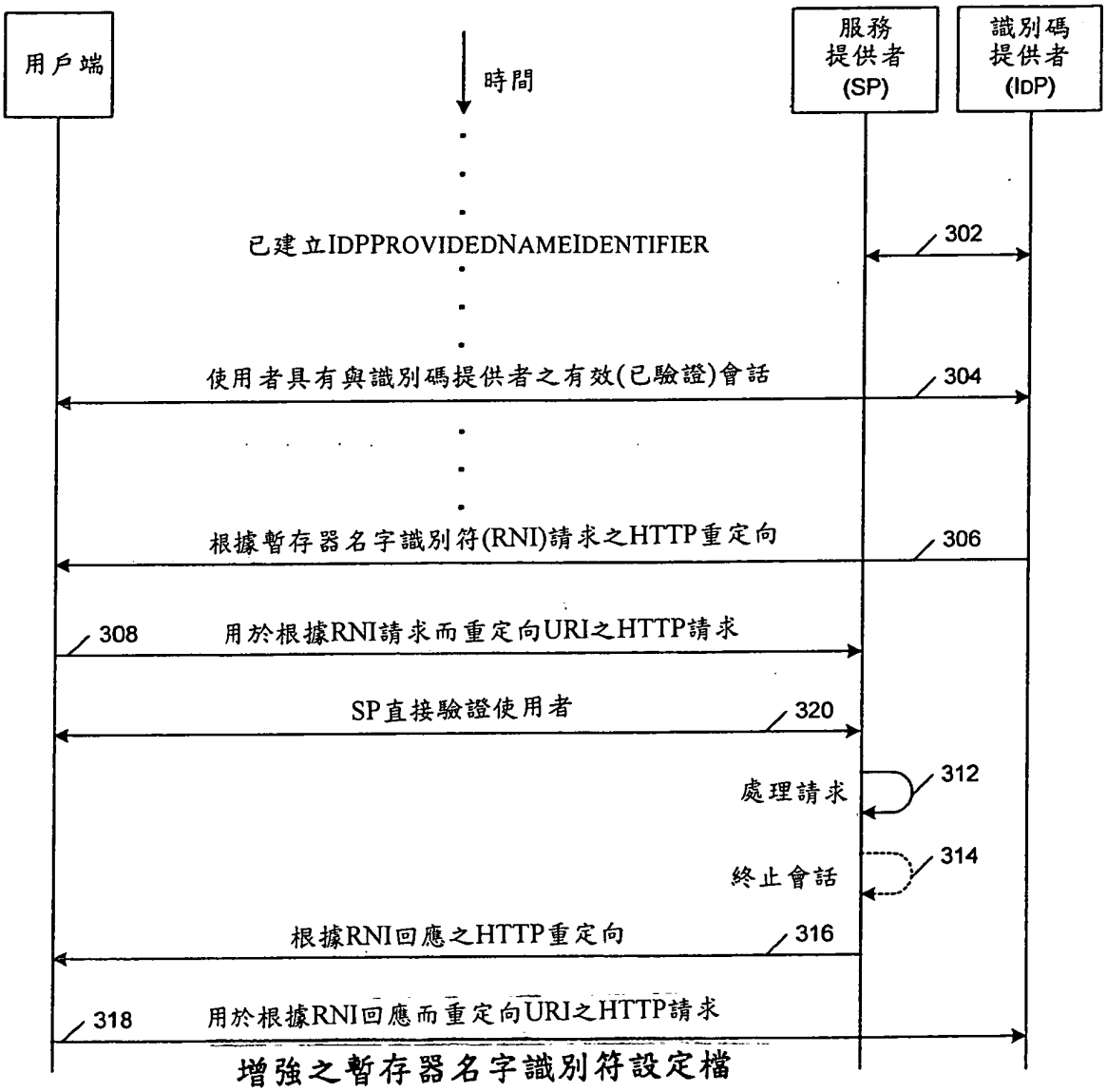


圖 2B
(先前技術)



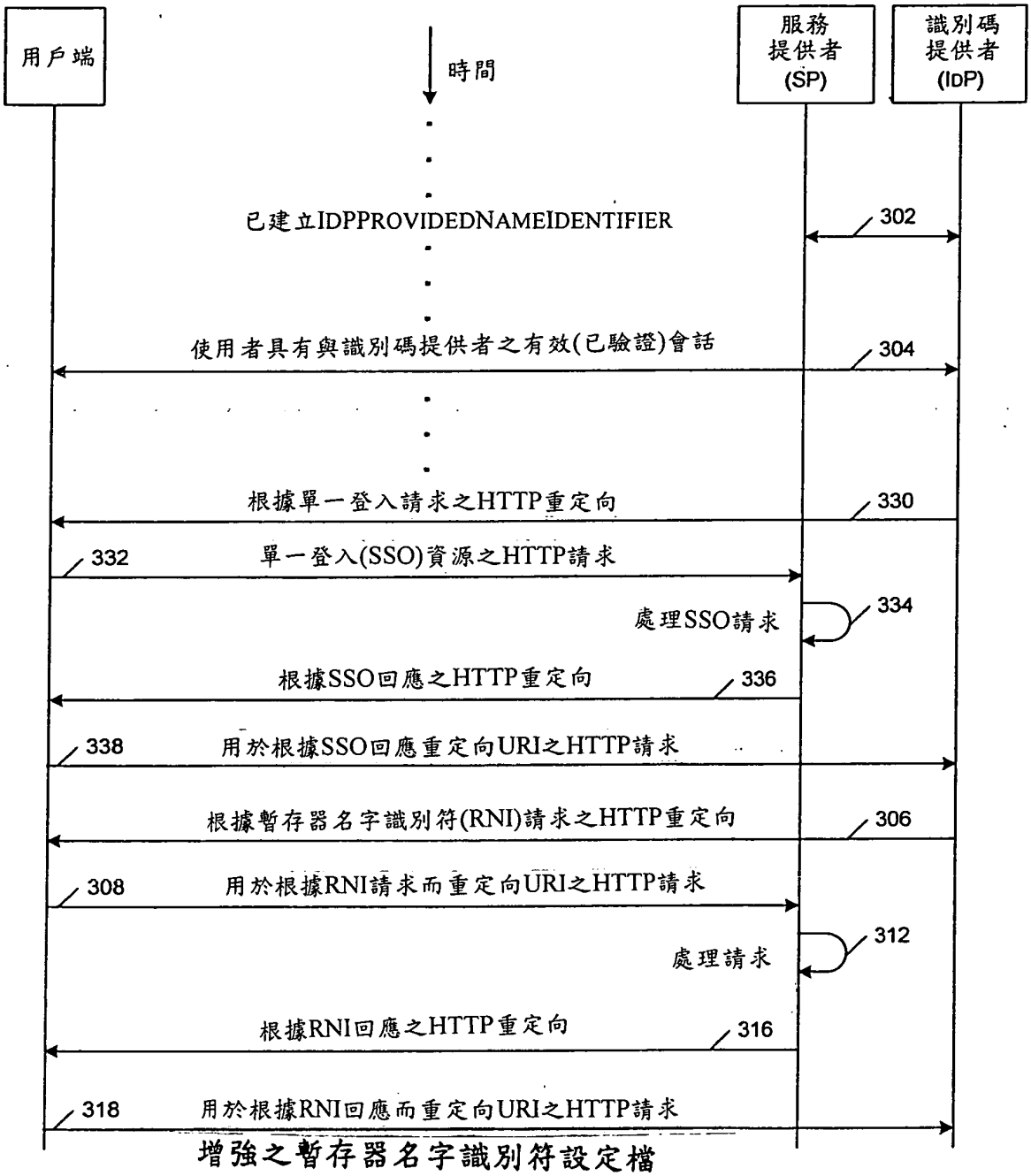
增強之暫存器名字識別符設定檔
(在識別碼提供者處初始化-一般化驗證)

圖 3A



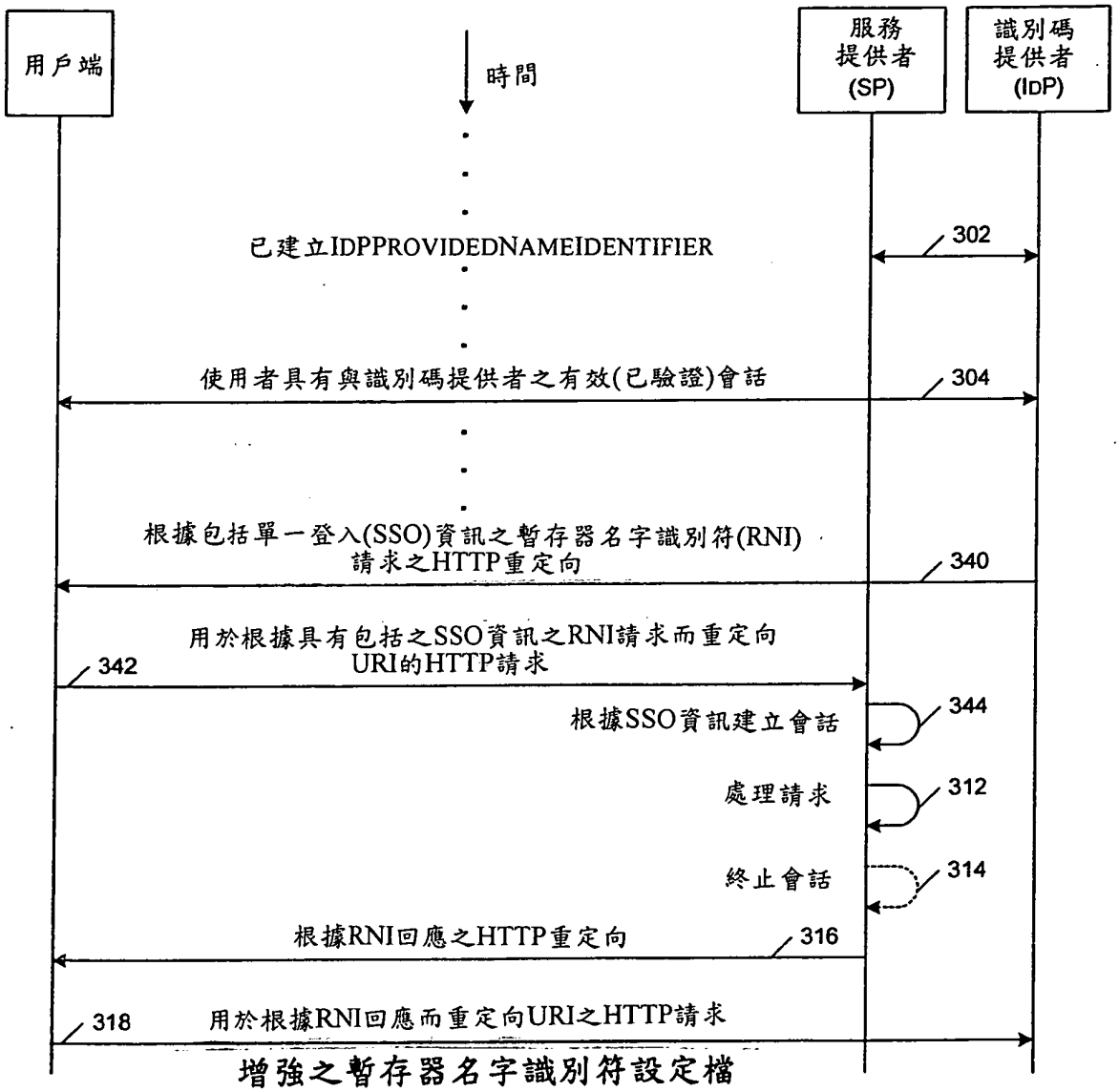
增強之暫存器名字識別符設定檔
(在識別碼提供者處初始化-直接驗證)

圖 3B



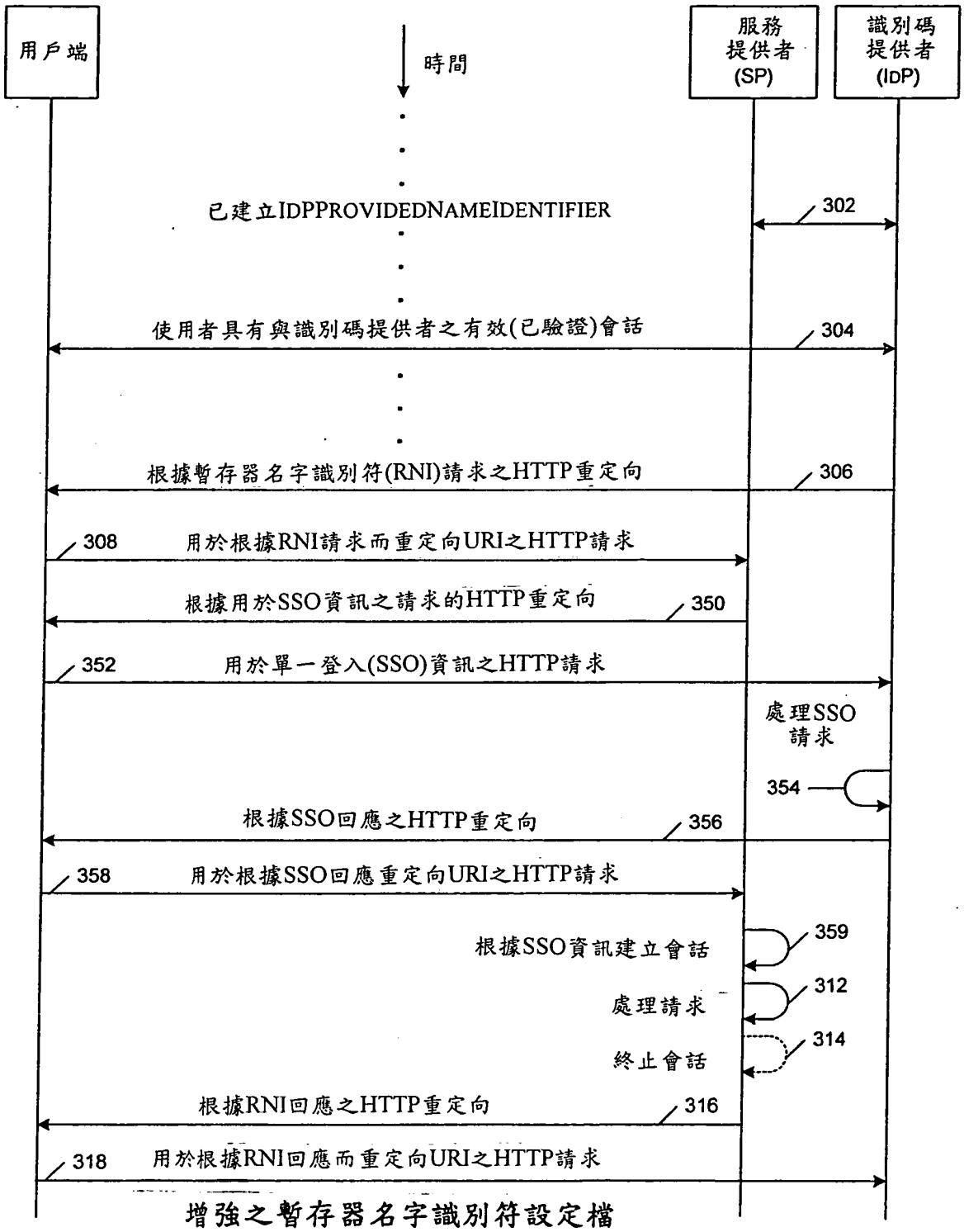
增強之暫存器名字識別符設定檔
(在識別碼提供者處初始化-初步單一登入)

圖 3C



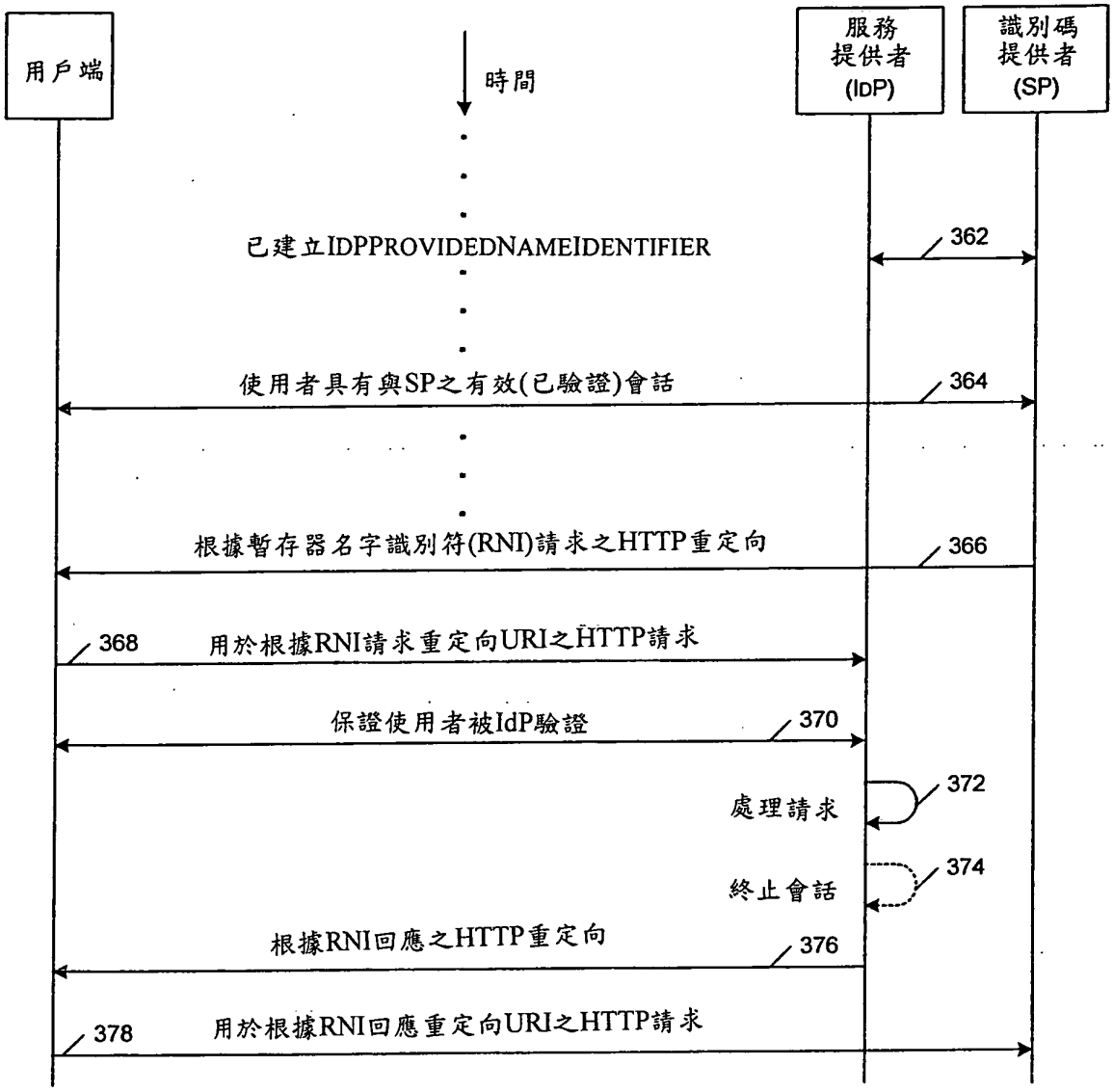
增強之暫存器名字識別符設定檔
(在識別碼提供者處初始化-推式單一登入)

圖 3D



增強之暫存器名字識別符設定檔
(在識別碼提供者處初始化-挽式單一登入)

圖 3E



增強之暫存器名字識別符設定檔(在服務提供者處初始化)

圖 3F

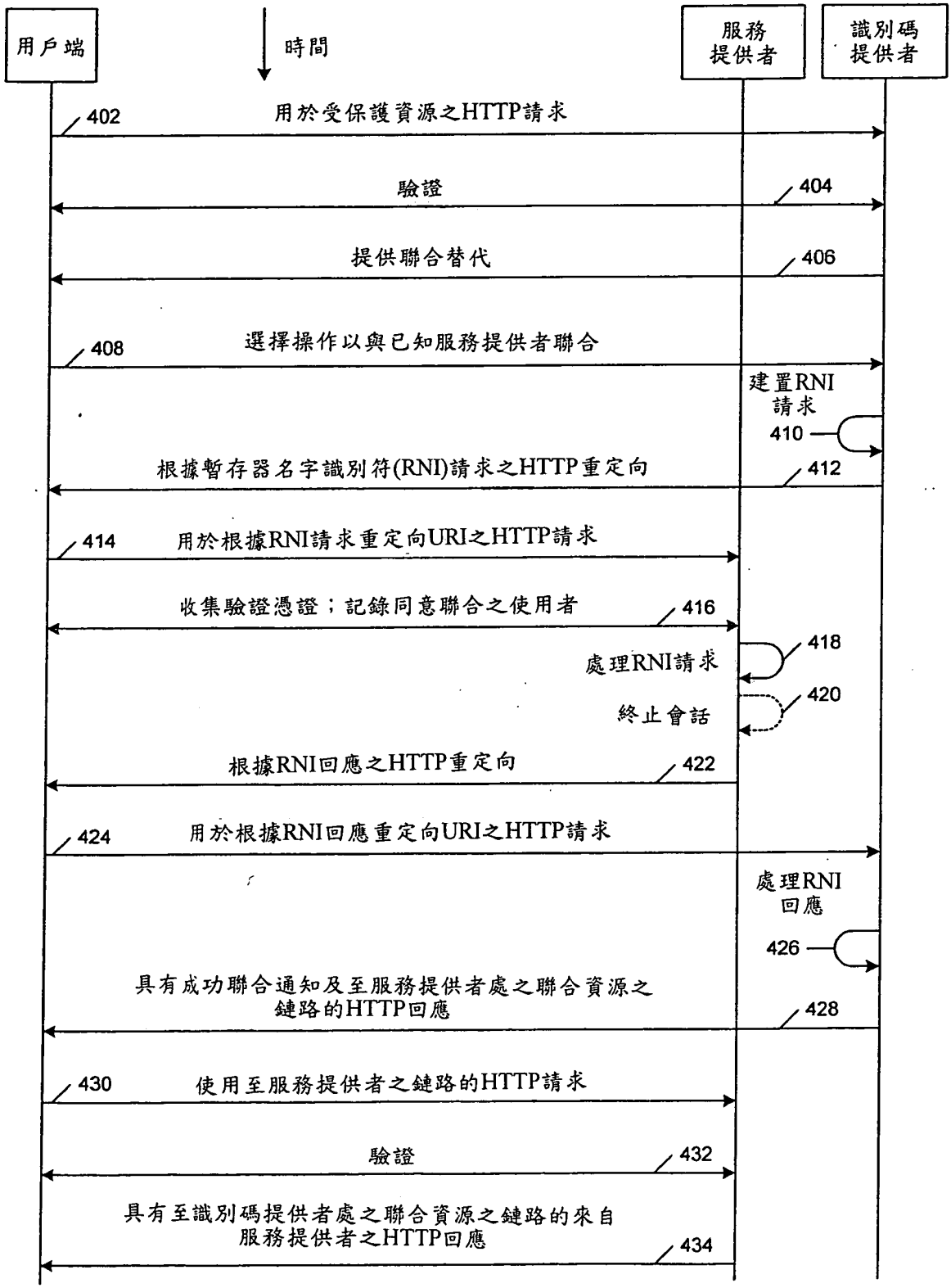

用戶端
時間
服務提供者
識別碼提供者
402
用於受保護資源之HTTP請求
驗證
404
提供聯合替代
406
408
選擇操作以與已知服務提供者聯合
建置RNI請求
410
根據暫存器名字識別符(RNI)請求之HTTP重定向
412
414
用於根據RNI請求重定向URI之HTTP請求
收集驗證憑證；記錄同意聯合之使用者
416
418
處理RNI請求
420
終止會話
根據RNI回應之HTTP重定向
422
424
用於根據RNI回應重定向URI之HTTP請求
處理RNI回應
426
具有成功聯合通知及至服務提供者處之聯合資源之鏈路的HTTP回應
428
430
使用至服務提供者之鏈路的HTTP請求
驗證
432
具有至識別碼提供者處之聯合資源之鏈路的來自服務提供者之HTTP回應
434

圖 4A

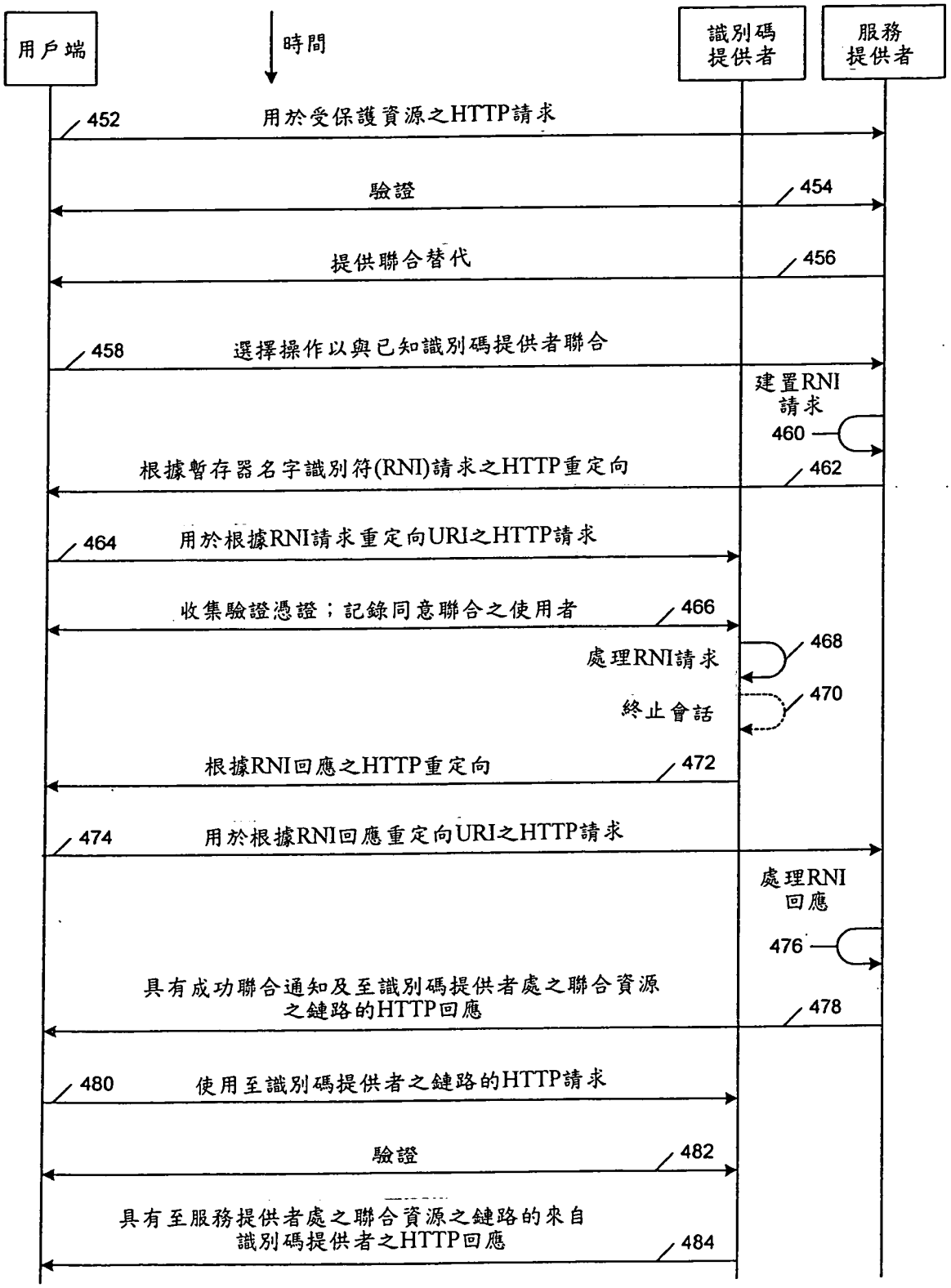

用戶端
時間
識別碼提供者
服務提供者
452
用於受保護資源之HTTP請求
驗證
454
提供聯合替代
456
458
選擇操作以與已知識別碼提供者聯合
建置RNI請求
460
根據暫存器名字識別符(RNI)請求之HTTP重定向
462
464
用於根據RNI請求重定向URI之HTTP請求
收集驗證憑證；記錄同意聯合之使用者
466
處理RNI請求
468
終止會話
470
根據RNI回應之HTTP重定向
472
474
用於根據RNI回應重定向URI之HTTP請求
處理RNI回應
476
具有成功聯合通知及至識別碼提供者處之聯合資源之鏈路的HTTP回應
478
480
使用至識別碼提供者之鏈路的HTTP請求
驗證
482
具有至服務提供者處之聯合資源之鏈路的來自識別碼提供者之HTTP回應
484

圖 4B

七、指定代表圖：

(一)本案指定代表圖為：第（ 3A ）圖。

(二)本代表圖之元件符號簡單說明:

（無元件符號說明）

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）

100年12月1日修正替換頁

十、申請專利範圍：

1. 一種用於在一聯合計算環境內執行一操作的方法，該方法包含：

在該聯合計算環境內於一第二聯合實體處接收來自一第一聯合實體的一用於一主要者之暫存器名字識別符(RNI)請求；

回應於接收該用於該主要者之暫存器名字識別符(RNI)請求，在該第二聯合實體處執行一用於該主要者之驗證操作；

回應於成功地完成該驗證操作，在該第二聯合實體處於一暫存器名字識別符設定檔內註冊或修正一來自該接收之暫存器名字識別符請求的名字識別符；及

自該第二聯合實體將一暫存器名字識別符(RNI)回應發送至該第一聯合實體。

2. 如請求項1之方法，其中該第一聯合實體係一識別碼提供者且該第二聯合實體係一服務提供者。

3. 如請求項1之方法，其中該第一聯合實體係一服務提供者且該第二聯合實體係一識別碼提供者。

4. 如請求項1之方法，其進一步包含：

將在該第一聯合實體處之一用於該主要者的第一帳戶與在該第二聯合實體處之一用於該主要者的第二帳戶鏈接，使得關於該第一聯合實體之資訊可藉由該第二聯合實體提供至該主要者。

5. 如請求項1之方法，其進一步包含：

將在該第一聯合實體處之一用於該主要者的第一帳戶與在該第二聯合實體處之一用於該主要者的第二帳戶鏈接，使得該第一聯合實體及該第二聯合實體可代表該主要者執行一單一登入操作。

6. 如請求項1之方法，其進一步包含：

藉由該第二聯合實體直接與該主要者相互作用以執行該驗證操作。

7. 如請求項1之方法，其進一步包含：

基於已自該第一聯合實體接收之單一登入資訊以及該暫存器名字識別符請求，在該第二聯合實體處執行一單一登入操作作為該驗證操作。

8. 如請求項1之方法，其進一步包含：

藉由該第二聯合實體自該第一聯合實體請求單一登入資訊以執行該驗證操作。

9. 如請求項1之方法，其進一步包含：

在於該第二聯合實體處接收該用於該主要者之暫存器名字識別符請求之前，在該第二聯合實體處自該第一聯合實體接收一單一登入請求。

10. 一種用於在一聯合計算環境內執行一操作的裝置，該裝置包含：

一處理器；

一電腦記憶體，其具有多個電腦程式指令，當該等電腦程式指令由該處理器執行時，實施如請求項1至請求項9之任一項之方法。

11. 一種在一電腦可讀媒體上之用於在一聯合計算環境內執行一操作的電腦程式產品，該電腦程式產品具有多個電腦程式指令，當該等電腦程式指令由一處理系統執行時，實施如請求項1至請求項9之任一項之方法。