【發明說明書】

【中文發明名稱】 用於登入的認證方法

【技術領域】

【0001】本發明是有關於一種認證方法，特別是指一種用於登入的認證方法。

【先前技術】

【0002】使用者登入電子信箱網站、購物網站，或社群網站時，通常都會被要求輸入帳號與密碼。然而，若該使用者在不同的網站註冊不同的帳號與密碼，則該使用者需要記憶多組帳號與密碼，導致該使用者可能會遺忘某個網站的帳號或密碼，而無法登入。

【0003】為方便該使用者登入多個網站，現有相關技術人員提出了例如OpenID的單一簽入(Single Sign On, SSO)的解決方法，其係透過一身分提供者(Identity Provider)儲存多筆使用者資料，在登入網站時，該使用者根據一認證碼提供一相關於該身分提供者的統一資源標誌符(Uniform Resource Identifier, URI)，以致網站根據該統一資源標誌符連結至該身分提供者，該身分提供者再提供相關於該使用者的使用者資料，以認證該使用者的身分，讓該使用者只需要記憶一組認證碼，即可登入所有支援OpenID的所

有網站。舉例來說，使用者Alice在身分提供者http://openid-provider.org處註冊了一認證碼，該認證碼例如為alice，則使用者Alice提供給網站的該統一資源標誌符為http://alice.openid-provider.org/。

【0004】然而，現有的身分提供者認證機制較為薄弱，容易發生該身分提供者因管理不當而讓駭客竊取使用者資料，一旦使用者資料被竊取，該等使用者資料可能會被盜用，而導致所有支援OpenID的網站可能被駭客以該等使用者資料登入。

【發明內容】

【0005】因此，本發明的目的，即在提供一種具有高安全性的用於登入的認證方法。

【0006】於是，本發明用於登入的認證方法，由一包含一認證伺服端的系統來實施，該認證伺服端、一使用端模組，及一廠商伺服端經由一第一通訊網路相互連接，該用於登入的認證方法包含一步驟(A)、一步驟(B)，及一步驟(C)。

【0007】在步驟(A)中，當該認證伺服端經由該第一通訊網路接收到一來自該廠商伺服端的連結請求時，該認證伺服端產生並儲存一伺服識別碼，且經由該第一通訊網路傳送該伺服識別碼至該廠商伺服端，以致該廠商伺服端經由該第一通訊網路傳送該伺服識別碼至

該使用端模組。

【0008】在步驟(B)中，當該認證伺服端經由該第一通訊網路從該使用端模組接收到一由該使用端模組根據一預存的變換金鑰加密該伺服識別碼而產生的加密伺服識別碼、一對應於該使用端模組與該變換金鑰的使用端序號，及一筆使用者資料時，該認證伺服端判定該加密伺服識別碼及該使用端序號的組合是否為已被授權。

【0009】在步驟(C)中，當該認證伺服端判定出該加密伺服識別碼及該使用端序號的組合為已被授權時，該認證伺服端經由該第一通訊網路傳送一授權登入通知及該使用者資料至該廠商伺服端。

【0010】本發明之功效在於：藉由該使用端模組根據該變換金鑰加密該伺服識別碼以產生該加密伺服識別碼，以致該認證伺服端進行該加密伺服識別碼及該使用端序號的組合是否為已被授權的判定，當該認證伺服端判定出該加密伺服識別碼及該使用端序號的組合為已被授權時，該認證伺服端才傳送該授權登入通知及該使用者資料至該廠商伺服端，藉此只需要該變換金鑰及該使用端序號，即可登入所有支援該認證伺服端的廠商伺服端，且該認證伺服端不儲存該使用者資料，以避免駭客駭入該認證伺服端竊取該使用者資料，提高安全性。

【圖式簡單說明】

【0011】本發明的其他的特徵及功效，將於參照圖式的實施方式中清楚地呈現，其中：

圖 1 是一方塊圖，示例地繪示一用來實施本發明用於登入的認證方法之一實施例的系統；

圖 2 是一流程圖，說明該實施例的一註冊程序；

圖 3 是一流程圖，說明該實施例的一登入程序；及

圖 4 是一流程圖，說明圖 3 中步驟 38 的子步驟。

【實施方式】

【0012】參閱圖1，圖1說明用來實施本發明用於登入的認證方法之一實施例的一系統100，包含一認證伺服端11、一廠商伺服端12，及一使用端模組13。

【0013】該認證伺服端11連接一第一通訊網路14，並儲存有多個初始金鑰、多個比對序號及多個分別對應該等比對序號的驗證金鑰，該第一通訊網路14例如是一網際網路。

【0014】該廠商伺服端12經由該第一通訊網路14與該認證伺服端11連接。

【0015】該使用端模組13包括一經由該第一通訊網路14與該廠商伺服端12連接的電腦裝置131、一經由該第一通訊網路14與該認證伺服端11連接且連接一第二通訊網路15的行動裝置132，及一經

由該第二通訊網路15與該行動裝置132連接的帳密保護器133，該帳密保護器133儲存有一使用端初始金鑰、一對應該帳密保護器133的使用端序號，及一筆使用者資料，該第二通訊網路15例如是一短距無線通訊網路。此外，在其他實施例中，該使用端模組13可不包括該電腦裝置131，且該行動裝置132還經由該第一通訊網路14與該廠商伺服端12連接。

【0016】本發明登入的認證方法之該實施例包含一註冊程序及一登入程序。

【0017】參閱圖1及圖2，該註冊程序包含步驟21~29。以下詳述各個步驟。

【0018】在步驟21中，該行動裝置132經由該第二通訊網路15傳送一資料提供請求至該帳密保護器133。

【0019】在步驟22中，該帳密保護器133回應於該資料提供請求，經由該第二通訊網路15傳送該使用端初始金鑰及該使用端序號至該行動裝置132。

【0020】在步驟23中，當該行動裝置132接收到該使用端初始金鑰及該使用端序號時，該行動裝置132經由該第一通訊網路14傳送該使用端初始金鑰至該認證伺服端11。

【0021】在步驟24中，當該認證伺服端11接收到該使用端初始金鑰時，該認證伺服端11判定該使用端初始金鑰是否匹配於該等初始

金鑰的其中一者。若該判定結果為肯定，該流程進行步驟25，否則結束。

【0022】在步驟25中，當該認證伺服端11判定出該使用端初始金鑰匹配於該等初始金鑰的其中一者時，該認證伺服端11產生並經由該第一通訊網路14傳送一認證碼至該行動裝置132。

【0023】在步驟26中，當該行動裝置132接收到該認證碼時，該行動裝置132根據認證碼產生一筆相關於該認證碼的認證資料，並經由該第一通訊網路14傳送一筆包含該認證資料、該使用端初始金鑰及該使用端序號的註冊資料至該認證伺服端11。

【0024】在步驟27中，當該認證伺服端11接收到該註冊資料時，該認證伺服端11根據該註冊資料的該認證資料判定該認證資料是否與該認證碼相符。若該判定結果為肯定，該流程進行步驟28，否則結束。

【0025】在步驟28中，當該認證伺服端11判定出該認證資料與該認證碼相符時，該認證伺服端11根據該註冊資料的該使用端初始金鑰產生一變換金鑰，並經由該第一通訊網路14傳送該變換金鑰至該行動裝置132，且根據該變換金鑰產生並儲存一對應該使用端序號且對應該變換金鑰的驗證金鑰，且將該使用端序號儲存為不同於該等比對序號的另一比對序號。值得注意的是，在本實施例中，該變換金鑰與該驗證金鑰相同，亦即該變換金鑰與該驗證金鑰用於對稱

加密。在其他實施例中該變換金鑰與該驗證金鑰不同，亦即該變換金鑰與該驗證金鑰用於非對稱加密，例如公開金鑰加密，其中該變換金鑰為一私鑰，且該驗證金鑰為一對應該變換金鑰的公鑰。

【0026】在步驟29中，當該行動裝置132接收到該變換金鑰時，該行動裝置132經由該第二通訊網路15傳送該變換金鑰至該帳密保護器133，以致該帳密保護器133儲存該變換金鑰。

【0027】參閱圖1及圖3，該登入程序包含步驟31~39。以下詳述各個步驟。

【0028】在步驟31中，該電腦裝置131經由該第一通訊網路14傳送一登入請求至該廠商伺服端12。要特別注意的是，在其他該使用端模組13不包含該電腦裝置131的實施例中，係由該行動裝置132經由該第一通訊網路14傳送一登入請求至該廠商伺服端12。

【0029】在步驟32中，當該廠商伺服端12接收到該登入請求時，該廠商伺服端12根據該登入請求產生一連結請求並經由該第一通訊網路14傳送該連結請求至該認證伺服端11。

【0030】在步驟33中，當該認證伺服端11接收到該連結請求時，該認證伺服端11產生並儲存一伺服識別碼，且經由該第一通訊網路14傳送該伺服識別碼至該廠商伺服端12。在本實施例中，該伺服識別碼例如是以快速響應矩陣碼(Quick Response code, QR code)編碼。

【0031】在步驟34中，當該廠商伺服端12接收到該伺服識別碼時，該廠商伺服端12經由該第一通訊網路14傳送該伺服識別碼至該電腦裝置131。

【0032】在步驟35中，該行動裝置132從該電腦裝置131獲得該伺服識別碼，並經由該第二通訊網路15傳送該伺服識別碼至該帳密保護器133。要再特別注意的是，在本實施例中，該行動裝置132是掃描該電腦裝置131所顯示的QR code以獲得該伺服識別碼，而在其他該使用端模組13不包含該電腦裝置131的實施例中，在步驟34該廠商伺服端12經由該第一通訊網路14傳送該伺服識別碼至該行動裝置132，在步驟35當該行動裝置132接收到該伺服識別碼時，經由該第二通訊網路15傳送該伺服識別碼至該帳密保護器133。

【0033】在步驟36中，當該帳密保護器133接收到該伺服識別碼時，該帳密保護器133根據該變換金鑰加密該伺服識別碼而產生一加密伺服識別碼，並經由該第二通訊網路15傳送該加密伺服識別碼、該使用者資料，及該使用端序號至該行動裝置132。值得注意的是，在本實施例中，該帳密保護器133係回應於一使用者於該帳密保護器133的輸入操作，以根據該變換金鑰加密該伺服識別碼而產生該加密伺服識別碼，換句話說，該帳密保護器133除了接收到該伺服識別碼外，還需要該使用者於該帳密保護器133進行輸入操作時，才會回應於該輸入操作來根據該變換金鑰加密該伺服識別碼

而產生該加密伺服識別碼，並經由該第二通訊網路15傳送該加密伺服識別碼、該使用者資料，及該使用端序號至該行動裝置132。

【0034】在步驟37中，當該行動裝置132接收到該加密伺服識別碼、該使用者資料，及該使用端序號時，該行動裝置132經由該第一通訊網路14傳送該加密伺服識別碼、該使用者資料，及該使用端序號至該認證伺服端11。

【0035】在步驟38中，當該認證伺服端11接收到該加密伺服識別碼、該使用端序號，及該使用者資料時，該認證伺服端11判定該加密伺服識別碼及該使用端序號的組合是否為已被授權。若該判定結果為肯定，該流程進行步驟39，否則結束。

【0036】再參閱圖4，進一步詳細說明該認證伺服端11所執行的步驟38包含以下子步驟。

【0037】在子步驟381中，該認證伺服端11經由該第一通訊網路14接收該加密伺服識別碼、該使用端序號，及該使用者資料。

【0038】在子步驟382中，該認證伺服端11根據該使用端序號判定該使用端序號是否匹配於該等比對序號的其中一者。若該判定結果為肯定，該流程進行步驟383，否則結束。

【0039】在子步驟383中，當該認證伺服端11判定出該使用端序號匹配於該等比對序號的其中一者時，該認證伺服端11判定匹配於該使用端序號的比對序號對應的驗證金鑰也對應該變換金鑰。

【0040】在子步驟384中，該認證伺服端11根據對應該變換金鑰的驗證金鑰解密該加密伺服識別碼，以產生一解密伺服識別碼。

【0041】在子步驟385中，該認證伺服端11判定是否自身儲存有與該解密伺服識別碼匹配的伺服識別碼。若該判定結果為肯定，該流程進行步驟39，否則結束。

【0042】在步驟39中，當該認證伺服端11在步驟38中判定出該加密伺服識別碼及該使用端序號的組合為已被授權時，亦即在子步驟385中判定出自身儲存有與該解密伺服識別碼匹配的伺服識別碼時，該認證伺服端11經由該第一通訊網路14傳送一授權登入通知及該使用者資料至該廠商伺服端12。

【0043】綜上所述，本發明用於登入的認證方法，藉由該帳密保護器133根據該變換金鑰加密該伺服識別碼以產生該加密伺服識別碼，該認證伺服端11進行該加密伺服識別碼及該使用端序號的組合是否為已被授權的判定，當該認證伺服端11判定出該加密伺服識別碼及該使用端序號的組合為已被授權時，該認證伺服端11才傳送該授權登入通知及該使用者資料至該廠商伺服端12，藉此只需要該變換金鑰及該使用端序號，即可登入所有支援該認證伺服端11的廠商伺服端12，且該認證伺服端11不儲存該使用者資料，以避免駭客駭入該認證伺服端11竊取該使用者資料，提高安全性，故確實能達成本發明的目的。

【0044】惟以上所述者，僅為本發明的實施例而已，當不能以此限定本發明實施的範圍，凡是依本發明申請專利範圍及專利說明書內容所作的簡單的等效變化與修飾，皆仍屬本發明專利涵蓋的範圍內。

【符號說明】

【0045】

100	系統
11	認證伺服端
12	廠商伺服端
13	使用端模組
131	電腦裝置
132	行動裝置
133	帳密保護器
14	第一通訊網路
15	第二通訊網路
21~29	步驟
31~39	步驟
381~385	子步驟

專利案號：106115412

公告本　申請日:106/05/10

I652594

IPC分類：G06F 21/31 (2013.01)
G06F 15/16 (2006.01)

【發明摘要】

【中文發明名稱】　用於登入的認證方法

【中文】

一種用於登入的認證方法，包含以下步驟：(A)當一認證伺服端接收到一來自一廠商伺服端的連結請求時，該認證伺服端產生並儲存一伺服識別碼，且傳送該伺服識別碼至該廠商伺服端，以致該廠商伺服端傳送該伺服識別碼至一使用端模組；(B)當該認證伺服端從該使用端模組接收到一加密伺服識別碼、一使用端序號，及一筆使用者資料時，該認證伺服端判定該加密伺服識別碼及該使用端序號的組合是否為已被授權；及(C)當該認證伺服端判定出該加密伺服識別碼及該使用端序號的組合為已被授權時，該認證伺服端傳送一授權登入通知及該使用者資料至該廠商伺服端。

【指定代表圖】：圖（3）。

【代表圖之符號簡單說明】

31~39　步驟

【發明申請專利範圍】

【第1項】 一種用於登入的認證方法，由一包含一認證伺服端的系統來實施，該認證伺服端、一使用端模組，及一廠商伺服端經由一第一通訊網路相互連接，該用於登入的認證方法包含以下步驟：

(A)當該認證伺服端經由該第一通訊網路接收到一來自該廠商伺服端的連結請求時，該認證伺服端產生並儲存一伺服識別碼，且經由該第一通訊網路傳送該伺服識別碼至該廠商伺服端，以致該廠商伺服端經由該第一通訊網路傳送該伺服識別碼至該使用端模組；

(B)當該認證伺服端經由該第一通訊網路從該使用端模組接收到一由該使用端模組根據一預存的變換金鑰加密該伺服識別碼而產生的加密伺服識別碼、一對應於該使用端模組的使用端序號，及一筆使用者資料時，該認證伺服端判定該加密伺服識別碼及該使用端序號的組合是否為已被授權；及

(C)當該認證伺服端判定出該加密伺服識別碼及該使用端序號的組合為已被授權時，該認證伺服端經由該第一通訊網路傳送一授權登入通知及該使用者資料至該廠商伺服端。

【第2項】 如請求項1所述的用於登入的認證方法，該使用端模組包括一經由該第一通訊網路與該廠商伺服端連接且連接一第二通訊網路的行動裝置，及一經由該第二通訊網路與該行動裝置連接的帳密保護器，該帳密保護器儲存有該變換

金鑰，其中，在步驟(A)中，該廠商伺服端根據所接收到的來自該行動裝置的一登入請求產生該連結請求並傳送該連結請求至該認證伺服端，且該廠商伺服端經由該第一通訊網路傳送該伺服識別碼至該行動裝置，該行動裝置經由該第二通訊網路傳送該伺服識別碼至該帳密保護器，以致在步驟(B)中，該帳密保護器根據該變換金鑰加密該伺服識別碼而產生該加密伺服識別碼。

【第3項】 如請求項1所述的用於登入的認證方法，該使用端模組包括一經由該第一通訊網路與該廠商伺服端連接的電腦裝置、一連接一第二通訊網路的行動裝置，及一經由該第二通訊網路與該行動裝置連接的帳密保護器，該帳密保護器儲存有該變換金鑰，其中，在步驟(A)中，該廠商伺服端根據所接收到的來自該電腦裝置的一登入請求產生並傳送該連結請求，且該廠商伺服端經由該第一通訊網路傳送該伺服識別碼至該電腦裝置，該行動裝置在從該電腦裝置獲得該伺服識別碼後，經由該第二通訊網路傳送該伺服識別碼至該帳密保護器，以致在步驟(B)中，該帳密保護器根據該變換金鑰加密該伺服識別碼而產生該加密伺服識別碼。

【第4項】 請求項2或3所述的用於登入的認證方法，該行動裝置還經由該第一通訊網路與該認證伺服端連接，該帳密保護器還儲存有對應該帳密保護器的該使用端序號及該使用者資料，其中，在步驟(B)中，該帳密保護器將該加密伺服識別碼、該使用端序號及該使用者資料經由該第二通訊網路

傳送至該行動裝置，該行動裝置再經由該第一通訊網路傳送該加密伺服識別碼、該使用端序號及該使用者資料至該認證伺服端。

【第5項】 如請求項1所述的用於登入的認證方法，該認證伺服端儲存有多個比對序號及多個分別對應該等比對序號的驗證金鑰，其中，步驟(B)包含以下子步驟：

(B-1)該認證伺服端經由該第一通訊網路接收該加密伺服識別碼、該使用端序號，及該使用者資料；

(B-2)當該認證伺服端接收到該加密伺服識別碼、該使用端序號，及該使用者資料時，該認證伺服端根據該使用端序號判定該使用端序號是否匹配於該等比對序號的其中一者；

(B-3)當該認證伺服端判定出該使用端序號匹配於該等比對序號的其中一者時，該認證伺服端判定匹配於該使用端序號的比對序號對應的驗證金鑰也對應該變換金鑰；

(B-4)該認證伺服端根據對應該變換金鑰的驗證金鑰解密該加密伺服識別碼，以產生一解密伺服識別碼；及

(B-5)該認證伺服端判定是否自身儲存有與該解密伺服識別碼匹配的伺服識別碼；

在步驟(C)中，當該認證伺服端判定出自身儲存有與該解密伺服識別碼匹配的伺服識別碼時，該認證伺服端判定該加密伺服識別碼及該使用端序號的組合為已被授權。

【第6項】 如請求項1所述的用於登入的認證方法，該認證伺服端儲

存有多個初始金鑰，該使用端模組儲存有一使用端初始金鑰，在步驟(A)前還包含以下步驟：

(D)當該認證伺服端經由該第一通訊網路接收到來自該使用端模組的該使用端初始金鑰時，該認證伺服端判定該使用端初始金鑰是否匹配於該等初始金鑰的其中一者；

(E)當該認證伺服端判定出該使用端初始金鑰匹配於該等初始金鑰的其中一者時，該認證伺服端產生並傳送一認證碼至該使用端模組，以致該使用端模組經由該第一通訊網路傳送一筆包含相關於該認證碼的認證資料、該使用端初始金鑰及該使用端序號的註冊資料至該認證伺服端；

(F)該認證伺服端根據該註冊資料的該認證資料判定該認證資料是否與該認證碼相符；及

(G)當該認證伺服端判定出該認證資料與該認證碼相符時，該認證伺服端根據該註冊資料的該使用端初始金鑰產生該變換金鑰，並經由該第一通訊網路傳送該變換金鑰至該使用端模組，且根據該變換金鑰產生並儲存一對應該使用端序號且對應該變換金鑰的驗證金鑰，且將該使用端序號儲存為一比對序號。

【第7項】 如請求項6所述的用於登入的認證方法，該使用端模組包括一連接該第一通訊網路及一第二通訊網路的行動裝置，及一經由該第二通訊網路與該行動裝置連接的帳密保護器，該行動裝置經由該第一通訊網路與該認證伺服端連

接，該帳密保護器儲存有該使用端初始金鑰，其中，在步驟(D)中，該帳密保護器回應於一來自該行動裝置的資料提供請求，經由該第二通訊網路傳送該使用端初始金鑰及該使用端序號至該行動裝置，該行動裝置經由該第一通訊網路傳送該使用端初始金鑰至該認證伺服端，在步驟(E)中，當該行動裝置經由該第一通訊網路接收到該認證碼時，該行動裝置根據該認證碼產生該認證資料，並經由該第一通訊網路傳送該註冊資料至該認證伺服端，在步驟(G)中，該行動裝置經由該第一通訊網路接收該變換金鑰，並經由該第二通訊網路傳送該變換金鑰至該帳密保護器。

【第8項】 如請求項2、3、7之任一項所述的用於登入的認證方法，其中，該第一通訊網路是一網際網路，該第二通訊網路是一短距無線通訊網路。

【第9項】 如請求項1所述的用於登入的認證方法，其中，在步驟(A)中，該伺服識別碼是以快速響應矩陣碼編碼。

【發明圖式】

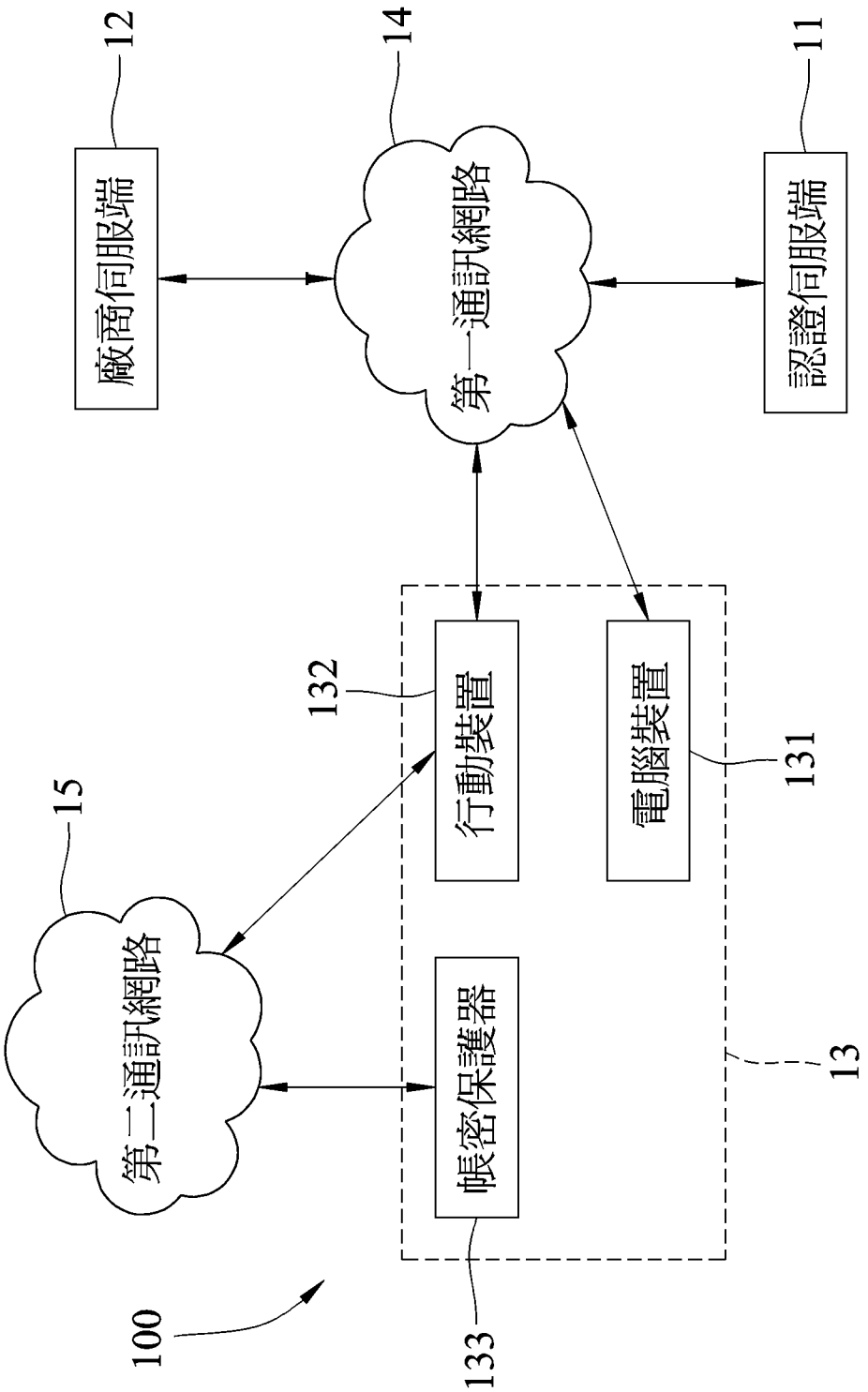
12
廠商伺服端
14
第一通訊網路
11
認證伺服端
132
行動裝置
131
電腦裝置
15
第二通訊網路
帳密保護器
13
100
133

圖1

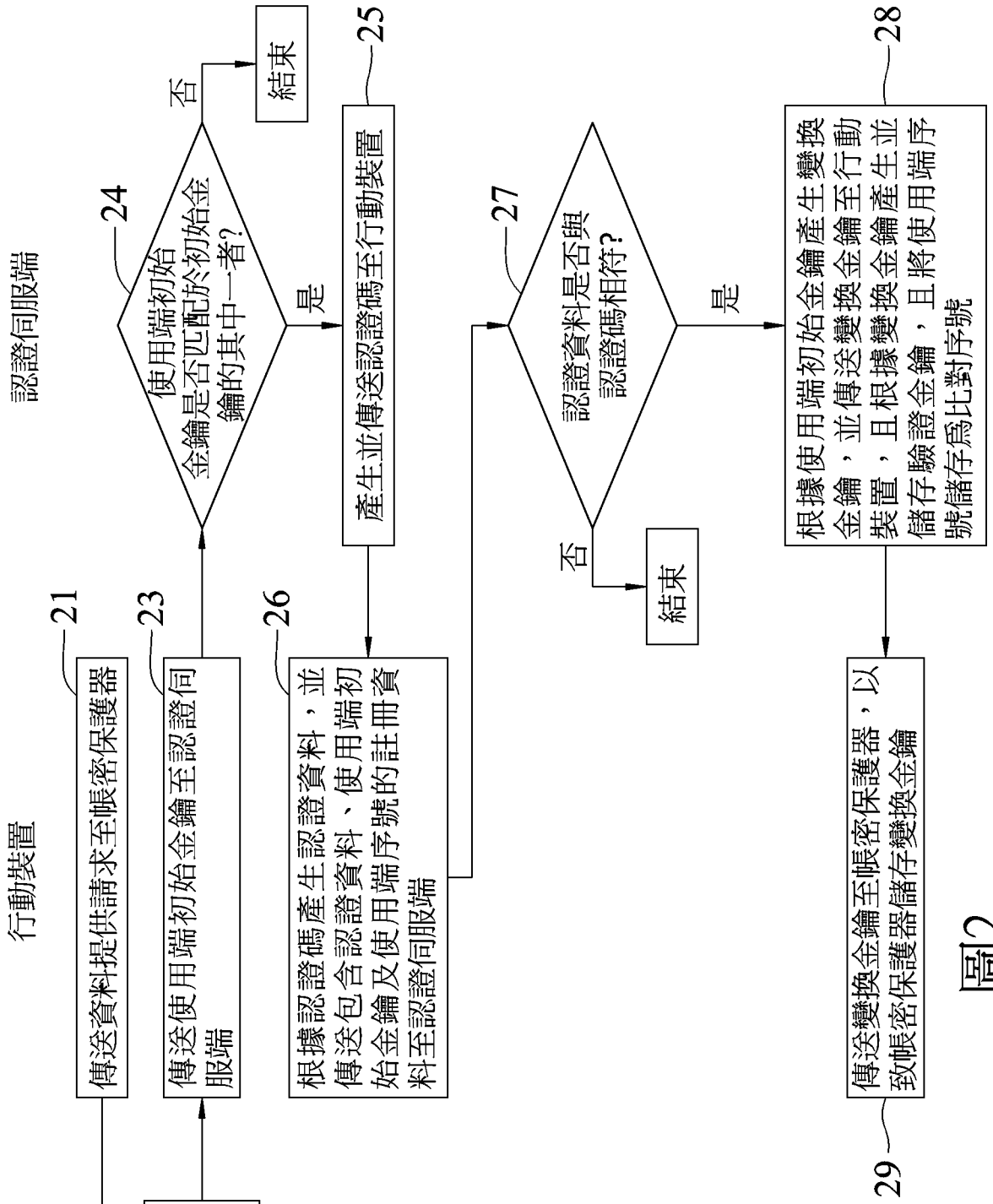
帳密保護器
行動裝置
認證伺服端
回應於資料提供請求，傳送使用端初始金鑰及該使用端序號至行動裝置
22
傳送資料提供請求至帳密保護器
21
傳送使用端初始金鑰至認證伺服端
23
使用端初始金鑰是否匹配於初始金鑰的其中一者?
24
否
結束
是
產生並傳送認證碼至行動裝置
25
根據認證碼產生認證資料，並傳送包含認證資料、使用端初始金鑰及使用端序號的註冊資料至認證伺服端
26
認證資料是否與認證碼相符?
27
否
結束
是
根據使用端初始金鑰產生變換金鑰，並傳送變換金鑰至行動裝置，且根據變換金鑰產生並儲存驗證金鑰，且將使用端序號儲存爲比對序號
28
傳送變換金鑰至帳密保護器，以致帳密保護器儲存變換金鑰
29

圖2

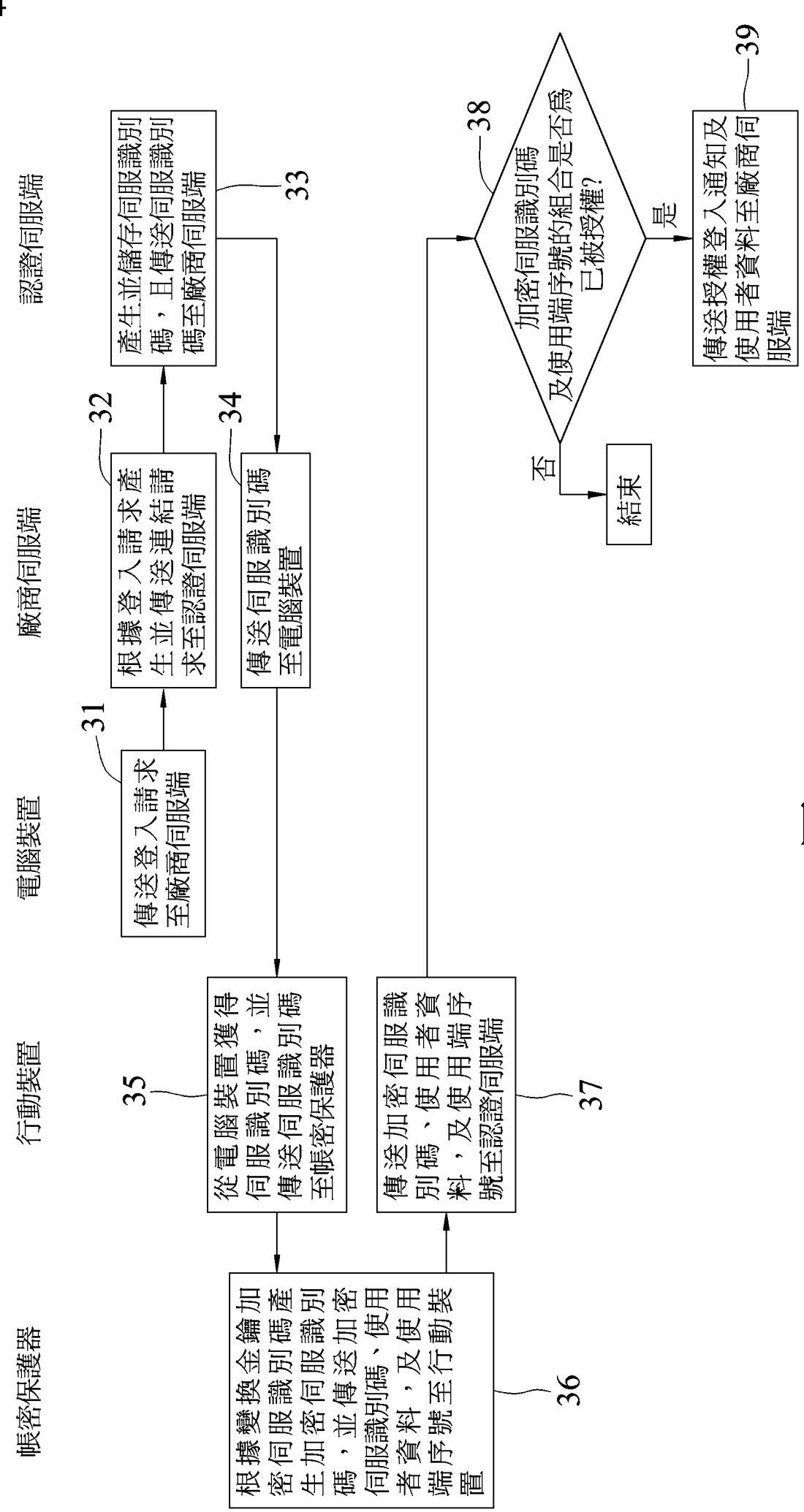
帳密保護器
行動裝置
電腦裝置
廠商伺服端
認證伺服端
傳送登入請求至廠商伺服端
31
根據登入請求產生並傳送連結請求至認證伺服端
32
產生並儲存伺服識別碼，且傳送伺服識別碼至廠商伺服端
33
傳送伺服識別碼至電腦裝置
34
從電腦裝置獲得伺服識別碼，並傳送伺服識別碼至帳密保護器
35
根據變換金鑰加密伺服識別碼產生加密伺服識別碼，並傳送加密伺服識別碼、使用者資料，及使用端序號至行動裝置
36
傳送加密伺服識別碼、使用者資料，及使用端序號至認證伺服端
37
加密伺服識別碼及使用端序號的組合是否爲已被授權?
38
是
否
結束
傳送授權登入通知及使用者資料至廠商伺服端
39

圖3

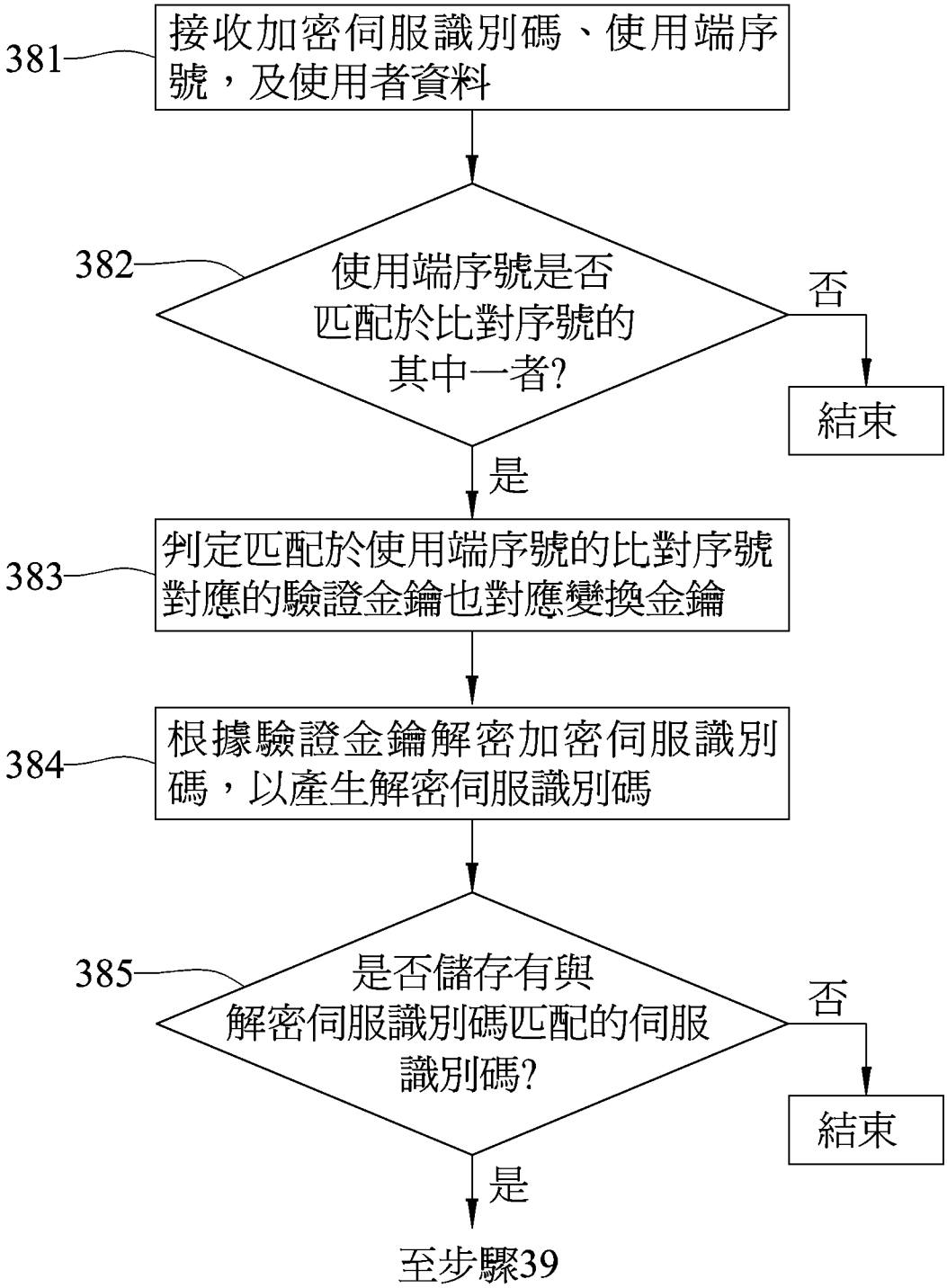
381
接收加密伺服識別碼、使用端序號，及使用者資料
382
使用端序號是否匹配於比對序號的其中一者?
否
結束
是
383
判定匹配於使用端序號的比對序號對應的驗證金鑰也對應變換金鑰
384
根據驗證金鑰解密加密伺服識別碼，以產生解密伺服識別碼
385
是否儲存有與解密伺服識別碼匹配的伺服識別碼?
否
結束
是
至步驟39

圖4