202037111

(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 202037111 A

(43)公開日： 中華民國 109 (2020) 年 10 月 01 日

(21)申請案號：108110157　(22)申請日： 中華民國 108 (2019) 年 03 月 22 日

(51)Int. Cl.：　*H04L9/32　(2006.01)*

(71)申請人：何六百有限公司 (中華民國) HO600 LTD.　(TW)

南投縣埔里鎮東潤路 42-7 號

(72)發明人：何岳峰 HO, YUEH-FENG (TW)

(74)代理人：何崇民

申請實體審查：有　申請專利範圍項數：12 項　圖式數：5　共 22 頁

(54)名稱

登錄認證方法

(57)摘要

一種登錄認證方法，與一金鑰驗證碼對應的成對公、私鑰分別儲存在服務提供者與使用者的電腦後，當該使用者欲在一登錄電腦登錄該服務時，服務提供者給予該使用者一隨機字串與一回傳簽章網址儲存至使用者的電腦，該使用者的電腦以私鑰將該隨機字串加密為一數位簽章後，傳輸至該回傳簽章網址供服務提供者電腦取得，服務提供者電腦以該公鑰解密驗證該隨機字串是否正確，若正確則令該使用者登錄該服務；藉由上述登錄認證的方法，使得使用者登錄服務時不需要背誦帳號與密碼，不會有遺失帳號密碼的問題，登錄的程序簡便且具有較高的安全性。

指定代表圖：

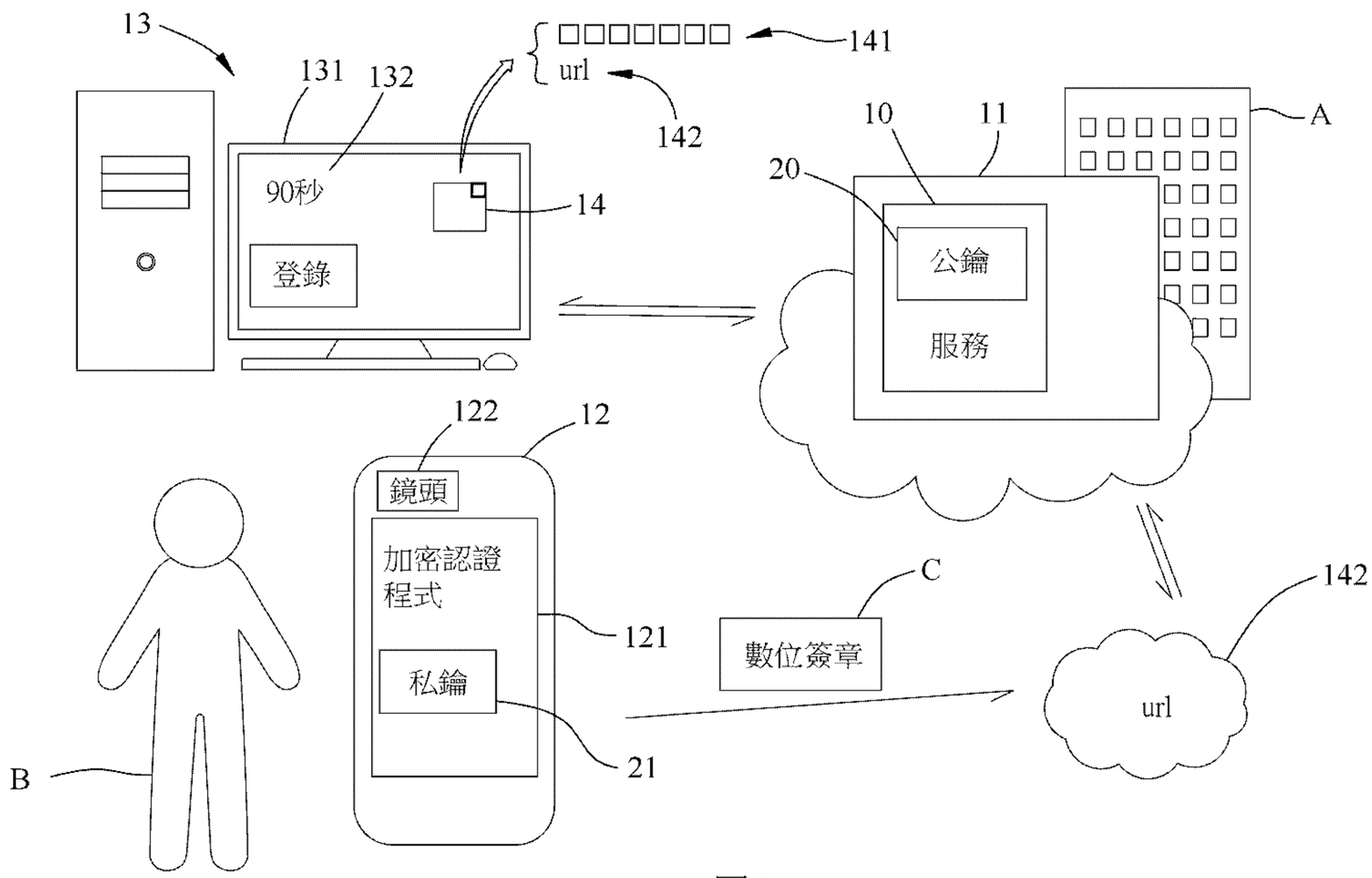


圖 1

符號簡單說明：

10:服務

11:服務提供者電腦

12:認證登錄電腦

121:加密認證程式

122:鏡頭

13:登錄電腦

131:顯示器

132:登錄時限

14:二維條碼

141:隨機字串

142:回傳簽章網址

20:公鑰

21:私鑰

A:服務提供者

B:使用者

C:數位簽章

申請日：
IPC 分類：

202037111

【發明摘要】

【中文發明名稱】　登錄認證方法

【中文】

一種登錄認證方法，與一金鑰驗證碼對應的成對公、私鑰分別儲存在服務提供者與使用者的電腦後，當該使用者欲在一登錄電腦登錄該服務時，服務提供者給予該使用者一隨機字串與一回傳簽章網址儲存至使用者的電腦，該使用者的電腦以私鑰將該隨機字串加密為一數位簽章後，傳輸至該回傳簽章網址供服務提供者電腦取得，服務提供者電腦以該公鑰解密驗證該隨機字串是否正確，若正確則令該使用者登錄該服務；藉由上述登錄認證的方法，使得使用者登錄服務時不需要背誦帳號與密碼，不會有遺失帳號密碼的問題，登錄的程序簡便且具有較高的安全性。

【指定代表圖】　圖1

【代表圖之符號簡單說明】

10服務　11服務提供者電腦

12認證登錄電腦　121加密認證程式

122鏡頭　13登錄電腦

131顯示器　132登錄時限

14二維條碼　141隨機字串

142回傳簽章網址　20公鑰

21私鑰　A服務提供者

B使用者　C數位簽章

【發明說明書】

【中文發明名稱】　登錄認證方法

【技術領域】

【0001】　本發明涉及一種非對稱金鑰的認證方法，尤其涉及一種登錄時取得字串加密為簽章登錄的登錄認證方法。

【先前技術】

【0002】　現有的網路服務，例如電子郵件、社群網站或者即時通訊軟體在登錄服務時，主要是以註冊服務時所得到的帳號與密碼在個人電腦或手機登錄上述的網路服務，帳號通常是設定為使用者的電子郵件信箱，在使用者註冊後服務提供者將對應帳號的密碼寄往使用者的電子郵件信箱，供使用者接收並在序登錄服務時使用。

【0003】　由於上述登錄網路服務的方式是以帳號、密碼的方式登錄服務，因此使用者需要在程式或網頁的介面中輸入帳號、密碼才能登錄服務，甚至有些人因為擔心遺忘帳號密碼而將帳號密碼寫在手札或筆記上，如此需要背誦帳號密碼的方式，除了使得登錄服務的過程較為麻煩以外，帳號密碼寫在札記或筆記上也容易被盜取而產生資訊安全上的問題。

【發明內容】

【0004】　由於現有登錄網路服務的方式需要使用帳號密碼，除了容易遺忘以外也容易被盜取造成安全性問題。為此，本發明利用成對的金鑰配合隨機字串的加解密，能夠達到安全且無需輸入帳號密碼的認證登錄效果。

【0005】　為達到上述目的，本發明提供一種服務提供者電腦端的登錄認證方法，其步驟包括：

【0006】　輸出隨機字串與網址：與一金鑰驗證碼對應的成對私鑰與公鑰分別儲存在一認證登錄電腦以及一服務提供者電腦，該服務提供者電腦提供一服務，該使用者欲於一登錄電腦登錄該服務時，該服務提供者電腦依該使用者要求給予一回傳簽章網址以及一隨機字串；

【0007】　接收數位簽章：該服務提供者電腦由該回傳簽章網址接收該認證登錄電腦回傳的一數位簽章，該數位簽章是該認證登錄電腦以該私鑰將該隨機字串加密而成，由該數位簽章能辨識出將其加密的該私鑰的金鑰驗證碼；以及

【0008】　認證登錄：該服務提供者電腦以對應該金鑰驗證碼的該公鑰解開該數位簽章，驗證該數位簽章內的該隨機字串與該服務提供者電腦給予使用者的該隨機字串是否相同，若相同則允許該使用者在該登錄電腦登錄該服務。

【0009】　較佳的，本發明在所述輸出隨機字串與網址的步驟中，所述服務提供者電腦在所述登錄電腦的一顯示器上顯示一二維條碼，該二維條碼的資訊包含所述的隨機字串與所述的回傳簽章網址，所述使用者在該認證登錄電腦執行一加密認證程式，利用該認證登錄電腦的一鏡頭拍攝、辨識該二維條碼取得該服務提供者電腦給予的該隨機字串與該回傳簽章網址；所述接收數位簽章的步驟中，該數位簽章是該認證登錄電腦執行該加密認證程式以該私鑰將該隨機字串加密而成。

【0010】　較佳的，本發明在所述輸出隨機字串與網址的步驟中，所述服務提供者電腦在所述登錄電腦的一顯示器上顯示所述的隨機字串與所述的回傳簽章網址，所述使用者在該認證登錄電腦執行一加密認證程式並將該隨機字串與該回傳簽章網址輸入該加密認證程式，借此取得該服務提供者電腦給予的該隨

機字串與該回傳簽章網址；所述接收數位簽章的步驟中，該數位簽章是該認證登錄電腦執行該加密認證程式以該私鑰將該隨機字串加密而成。

【0011】 較佳的，本發明在所述輸出隨機字串與網址的步驟中，所述服務提供者電腦在所述登錄電腦的一顯示器上顯示提供所述使用者輸入的一手機號碼欄位或一電子信箱欄位；當所述認證登錄電腦是手機並且該使用者將手機號碼輸入該手機號碼欄位後，所述服務提供者電腦以簡訊將所述的隨機字串與所述的回傳簽章網址寄給該認證登錄電腦，使該認證登錄電腦取得該服務提供者電腦給予的該隨機字串與該回傳簽章網址；以及當使用者將該認證登錄電腦能接收的電子信箱輸入該電子信箱欄位後，該服務提供者電腦以電子郵件將所述的隨機字串與所述的回傳簽章網址寄給該認證登錄電腦，使該認證登錄電腦取得該服務提供者電腦給予的該隨機字串與該回傳簽章網址；在所述接收數位簽章的步驟中，該數位簽章是該認證登錄電腦執行一加密認證程式以該私鑰將該隨機字串加密而成。

【0012】 較佳的，本發明在所述輸出隨機字串與網址的步驟中，所述服務提供者電腦在所述登錄電腦的一顯示器上顯示提供所述使用者輸入的一認證服務網址欄位；所述認證登錄電腦是伺服器並且執行一加密認證程式提供網路上的認證服務，當使用者將該認證服務的認證服務網址輸入該認證服務網址欄位後，該服務提供者電腦以查詢字串的方式將所述的隨機字串與所述的回傳簽章網址重導到認證服務網址，使該認證登錄電腦由該認證服務網址取得該服務提供者電腦給予的該隨機字串與該回傳簽章網址；所述接收數位簽章的步驟中，該數位簽章是該認證登錄電腦執行該加密認證程式以該私鑰將該隨機字串加密而成。

【0013】 本發明又提供一種認證登錄電腦端的登錄認證方法，其步驟包括：

【0014】　接收隨機字串與網址：與一金鑰驗證碼對應的成對私鑰與公鑰分別儲存在一認證登錄電腦以及一服務提供者電腦，該認證登錄電腦的使用者是該服務提供者電腦提供的一服務的使用者，當該使用者欲於一登錄電腦登錄該服務時，該服務提供者電腦依該使用者的要求給予一回傳簽章網址以及一隨機字串，該認證登錄電腦接收該回傳簽章網址以及該隨機字串；

【0015】　輸出數位簽章：該認證登錄電腦以該私鑰將該隨機字串加密為一數位簽章，由該數位簽章能辨識出將其加密的該私鑰的金鑰驗證碼，將該數位簽章輸出至該回傳簽章網址；以及

【0016】　被認證登錄：該數位簽章被該服務提供者電腦由該回傳簽章網址取得並以對應該金鑰驗證碼的該公鑰解開，若驗證該數位簽章內的該隨機字串與該服務提供者電腦給予使用者的該隨機字串相同，則允許該使用者在該登錄電腦登錄該服務。

【0017】　較佳的，本發明在所述接收隨機字串與網址的步驟中，所述服務提供者電腦在所述登錄電腦的一顯示器上顯示一二維條碼，該二維條碼的資訊包含所述的隨機字串與所述的回傳簽章網址，所述使用者在該認證登錄電腦執行一加密認證程式，利用該認證登錄電腦的一鏡頭拍攝、辨識該二維條碼取得該服務提供者電腦給予的該隨機字串與該回傳簽章網址；所述輸出數位簽章的步驟中，該數位簽章是該認證登錄電腦執行該加密認證程式以該私鑰將該隨機字串加密而成。

【0018】　較佳的，本發明在所述接收隨機字串與網址的步驟中，所述服務提供者電腦在所述登錄電腦的一顯示器上顯示所述的隨機字串與所述的回傳簽章網址，所述使用者在該認證登錄電腦執行一加密認證程式並將該隨機字串與該回傳簽章網址輸入該加密認證程式，借此取得該服務提供者電腦給予的該隨

機字串與該回傳簽章網址；所述輸出數位簽章的步驟中，該數位簽章是該認證登錄電腦執行該加密認證程式以該私鑰將該隨機字串加密而成。

【0019】 較佳的，本發明在所述接收隨機字串與網址的步驟中，所述服務提供者電腦在所述登錄電腦的一顯示器上顯示提供所述使用者輸入的一手機號碼欄位或一電子信箱欄位；當所述認證登錄電腦是手機並且該使用者將手機號碼輸入該手機號碼欄位後，所述服務提供者電腦以簡訊將所述的隨機字串與所述的回傳簽章網址寄給該認證登錄電腦，使該認證登錄電腦取得該服務提供者電腦給予的該隨機字串與該回傳簽章網址；以及當使用者將該認證登錄電腦能接收的電子信箱輸入該電子信箱欄位後，該服務提供者電腦以電子郵件將所述的隨機字串與所述的回傳簽章網址寄給該認證登錄電腦，使該認證登錄電腦取得該服務提供者電腦給予的該隨機字串與該回傳簽章網址；在所述輸出數位簽章的步驟中，該數位簽章是該認證登錄電腦執行一加密認證程式以該私鑰將該隨機字串加密而成。

【0020】 較佳的，本發明在所述接收隨機字串與網址的步驟中，所述服務提供者電腦在所述登錄電腦的一顯示器上顯示提供所述使用者輸入的一認證服務網址欄位；所述認證登錄電腦是伺服器並且執行一加密認證程式提供網路上的認證服務，當使用者將該認證服務的認證服務網址輸入該認證服務網址欄位後，該服務提供者電腦以查詢字串的方式將所述的隨機字串與所述的回傳簽章網址重導到認證服務網址，使該認證登錄電腦由該認證服務網址取得該服務提供者電腦給予的該隨機字串與該回傳簽章網址；所述輸出數位簽章的步驟中，該數位簽章是該認證登錄電腦執行該加密認證程式以該私鑰將該隨機字串加密而成。

【0021】 本發明的功效在於，透過本發明的方法能讓服務提供者電腦給予認證登錄電腦隨機字串與回傳簽章網址，利用私鑰加密隨機字串為數位簽章

後，回傳至該回傳簽章網址供服務提供者電腦取得並進行使用者的身份驗證，過程加密且能在當下由隨機字串的比對，確認請求登錄服務者是否是對應金鑰驗證碼的該服務的使用者，讓使用者無需在登錄電腦輸入帳號、密碼，即可由成對的公鑰、私鑰加解密該隨機字串的方式，讓使用者在任一登錄電腦上登錄該服務，避免背誦帳號、密碼的不便以及帳號、密碼容易遺失可能造成的安全性問題。

【圖式簡單說明】

【0022】

圖1是本發明第一較佳實施例方法的示意圖。

圖2是本發明第一較佳實施例該服務提供者端的流程圖。

圖3是本發明第一較佳實施例該使用者端的流程圖。

圖4是本發明第二較佳實施例方法的示意圖。

圖5是本發明第三較佳實施例方法的示意圖。

【實施方式】

【0023】 為能詳細瞭解本發明的技術特徵及實用功效，並可依照說明書的內容來實施，進一步以如圖式所示的較佳實施例，詳細說明如下。

【0024】 請參看如圖1至圖3所示的本發明第一較佳實施例，是提供一種登錄認證方法，用以登錄一服務提供者A提供的網路的服務10，例如電子郵件、社群網站、即時通訊軟體、購物網站、集資網站或網路論壇的服務。

【0025】 上述的服務10是架設在一服務提供者電腦11，例如伺服器或雲端的虛擬伺服器，當一使用者B註冊該服務時是先以一認證登錄電腦12例如手機或平板，以該認證登錄電腦12網路瀏覽器執行的加解密程式，或預先安裝在該認

證登錄電腦12的一加密認證程式121連上該服務10進行帳號的註冊，在註冊過程中產生與一金鑰驗證碼(Key ID)對應且成對的公鑰20與私鑰21，其中公鑰20儲存在該服務提供者電腦11，該服務提供者A能以該金鑰驗證碼辨識該使用者B的身分以及對應該使用者B的公鑰20，該私鑰21則儲存在該認證登錄電腦12而能供該加密認證程式121使用。

【0026】 如圖1至圖2所示，在使用者B註冊該服務10之後，本較佳實施例的該服務提供者A接受使用者B登錄該服務10的步驟S01至步驟S03包括：

【0027】 （S01）輸出隨機字串與網址：與一金鑰驗證碼(Key ID)對應的成對私鑰21與公鑰20已分別儲存在該認證登錄電腦12以及該服務提供者電腦11，該服務提供者電腦11提供一網路的服務10，該認證登錄電腦12執行一加密認證程式121。

【0028】 當使用者B要在某一登錄電腦13透過網路登錄該服務10時，該服務提供者電腦11依使用者B在該登錄電腦13上的要求，例如在該登錄電腦13的網路瀏覽器登錄該服務10時觸發登錄的要求，使得該服務提供者電腦11在一登錄時限132，例如90秒內於該登錄電腦13的顯示器131上顯示一二維條碼14，例如QR Code，該二維條碼14的資訊包含一隨機字串141與一回傳簽章網址142，每次登錄時限132內或分別刷新登錄網頁時產生在該顯示器131的二維條碼14所包含的隨機字串141不同。接著使用者B執行該加密認證程式121，利用該認證登錄電腦12的鏡頭122拍攝該二維條碼14，辨識後自動取得該服務提供者電腦11給予的該隨機字串141與該回傳簽章網址142。

【0029】 （S02）接收數位簽章：該服務提供者電腦11由網路接收該認證登錄電腦12回傳至該回傳簽章網址142的一數位簽章C，該數位簽章C是該認證登錄電腦12執行該加密認證程式121以該私鑰21加密該隨機字串141而成，由該數位簽章C能辨識出將其加密的該私鑰的金鑰驗證碼。

【0030】 （S03）認證登錄：該服務提供者電腦11以對應該金鑰驗證碼的該公鑰20解開該數位簽章C，驗證該數位簽章C內的該隨機字串141與該服務提供者電腦11當次的登錄時限132所輸出的該隨機字串141是否相同，若相同則允許該使用者B在該登錄電腦13登錄該服務10，若不同則拒絕該使用者B在該登錄電腦13登錄該服務10。

【0031】 如圖1、圖3所示，在使用者B註冊該服務10之後，該使用者B登錄該服務10的步驟S04至步驟S06包括：

【0032】 （S04）接收隨機字串與網址：與一金鑰驗證碼(Key ID)對應的成對私鑰21與公鑰20已分別儲存在該認證登錄電腦12以及該服務提供者電腦11，該使用者B為該服務提供者電腦11提供的一網路的服務10的使用者，且該認證登錄電腦12已安裝一加密認證程式121；該服務提供者電腦11依使用者B在某一登錄電腦13發出的登錄該服務10的要求，在一登錄時限132例如90秒內，於該登錄電腦13的顯示器131上顯示一二維條碼14，例如 QR Code，該二維條碼14的資訊包含一隨機字串141與一回傳簽章網址142，每次登錄時限132或刷新登錄網頁時所產生的隨機字串141會逐次更新；使用者B透過執行該加密認證程式121驅動該認證登錄電腦12的鏡頭122拍攝辨識該二維條碼14，辨識後獲得該服務提供者電腦11給予的該隨機字串141與該回傳簽章網址142。

【0033】 （S05）輸出數位簽章：該認證登錄電腦12執行的該加密認證程式121在取得該隨機字串141後，以該私鑰21將該隨機字串141加密為一數位簽章C，由該數位簽章C能辨識出將其加密的該私鑰的金鑰驗證碼，透過網路將該數位簽章C輸出至該回傳簽章網址142，供該服務提供者電腦11取得。

【0034】 （S06）被認證登錄：該數位簽章C被該服務提供者電腦11以對應該金鑰驗證碼的該公鑰20解開，驗證該數位簽章C內的該隨機字串141與該服務提供者電腦11當次的登錄時限132所輸出的該隨機字串141是否相同，若相同

則允許該使用者B在該登錄電腦13登錄該服務10，若不同則拒絕該使用者B在該登錄電腦13登錄該服務10。

【0035】　本發明除前述第一較佳實施例，在進行該輸出隨機字串與網址的步驟（S01）或該接收隨機字串與網址的步驟（S04）時，是以該認證登錄電腦12的鏡頭122拍攝該二維條碼14，辨識後取得該服務提供者電腦11給予的該隨機字串141與該回傳簽章網址142以外，該服務提供者電腦11於該登錄電腦13的顯示器131上顯示的二維條碼14，也能透過網路硬碟、藍牙傳輸、SD卡轉存等手段，將該二維條碼14的數位影像傳輸給該認證登錄電腦12的該加密認證程式121讀取，使該加密認證程式121辨識該二維條碼14的數位影像後，取得該服務提供者電腦11給予的該隨機字串141與該回傳簽章網址14。或者如以下所述的第二較佳實施例或第三較佳實施例，依使用者B的要求，該服務提供者電腦11可透過其他手段給予該隨機字串141與該回傳簽章網址142。

【0036】　如圖4所示的第二較佳實施例，該服務提供者電腦11依使用者B在該登錄電腦13上的要求，在所述的登錄時限132內於該登錄電腦13的顯示器131上顯示所述的隨機字串141與所述的回傳簽章網址142，每次登錄時限132或刷新登錄網頁時所產生的隨機字串141會逐次更新；使用者B將該隨機字串141與該回傳簽章網址142輸入該加密認證程式121，使該認證登錄電腦12手動地取得該服務提供者電腦11給予的該隨機字串141與該回傳簽章網址142，提供該加密認證程式121在後續的步驟（S02）或步驟（S05）執行使用。

【0037】　如圖5所示的第三較佳實施例，該服務提供者電腦11依使用者B在該登錄電腦13上的要求，在該登錄電腦13的顯示器13上顯示提供使用者B輸入的手機號碼欄位30（若該認證登錄電腦12為手機）、電子信箱欄位31，或認證服務網址欄位32（若該認證登錄電腦12是伺服器，且執行所述加密認證程式121提供網路上的認證服務）。

【0038】　首先，當使用者B將該認證登錄電腦12（即手機）的手機號碼輸入該手機號碼欄位30後，該服務提供者電腦11以簡訊的方式將所述的隨機字串141與所述的回傳簽章網址142寄給該認證登錄電腦12，使該認證登錄電腦12自動地取得該服務提供者電腦11給予的該隨機字串141與該回傳簽章網址142，提供所述的加密認證程式121在後續的步驟（S02）或步驟（S05）執行使用。

【0039】　其次，當使用者B將該認證登錄電腦12能接收的電子信箱輸入該電子信箱欄位31後，該服務提供者電腦11以電子郵件的方式將所述的隨機字串141與所述的回傳簽章網址142寄給該認證登錄電腦12，使該認證登錄電腦12自動地取得該服務提供者電腦11給予的該隨機字串141與該回傳簽章網址142，提供所述的加密認證程式121在後續的步驟（S02）或步驟（S05）執行使用。

【0040】　再者，當使用者B將該認證登錄電腦12（即伺服器）執行該加密認證程式121的認證服務網址輸入該認證服務網址欄位32後，該服務提供者電腦11以查詢字串（QueryString）的方式將所述的隨機字串141與所述的回傳簽章網址142重導到認證服務網址，使該認證登錄電腦12由該認證服務網址自動地取得該服務提供者電腦11給予的該隨機字串141與該回傳簽章網址142，提供所述的加密認證程式121在後續的步驟（S02）或步驟（S05）執行使用。

【0041】　以上所述僅為本發明的較佳實施例而已，並非用以限定本發明主張的權利範圍，凡其它未脫離本發明所揭示的精神所完成的等效改變或修飾，均應包括在本發明的申請專利範圍內。

【符號說明】

【0042】

S01步驟　　S02步驟

S03步驟　　S04步驟

S05步驟

S06步驟

10服務

11服務提供者電腦

12認證登錄電腦

121加密認證程式

122鏡頭

13登錄電腦

131顯示器

132登錄時限

14二維條碼

141隨機字串

142回傳簽章網址

20公鑰

21私鑰

A服務提供者

B使用者

C數位簽章

30手機號碼欄位

31電子信箱欄位

32認證服務網址欄位

【發明申請專利範圍】

【第1項】 一種登錄認證方法，其步驟包括：

輸出隨機字串與網址：與一金鑰驗證碼對應的成對私鑰與公鑰分別儲存在一認證登錄電腦以及一服務提供者電腦，該服務提供者電腦提供一服務，該使用者欲於一登錄電腦登錄該服務時，該服務提供者電腦依該使用者要求給予一回傳簽章網址以及一隨機字串；

接收數位簽章：該服務提供者電腦由該回傳簽章網址接收該認證登錄電腦回傳的一數位簽章，該數位簽章是該認證登錄電腦以該私鑰將該隨機字串加密而成，由該數位簽章能辨識出將其加密的該私鑰的金鑰驗證碼；以及

認證登錄：該服務提供者電腦以對應該金鑰驗證碼的該公鑰解開該數位簽章，驗證該數位簽章內的該隨機字串與該服務提供者電腦給予使用者的該隨機字串是否相同，若相同則允許該使用者在該登錄電腦登錄該服務。

【第2項】 如請求項1之登錄認證方法，其中在所述輸出隨機字串與網址的步驟中，所述服務提供者電腦在所述登錄電腦的一顯示器上顯示一二維條碼，該二維條碼的資訊包含所述的隨機字串與所述的回傳簽章網址，所述使用者在該認證登錄電腦執行一加密認證程式，利用該認證登錄電腦的一鏡頭拍攝、辨識該二維條碼取得該服務提供者電腦給予的該隨機字串與該回傳簽章網址；所述接收數位簽章的步驟中，該數位簽章是該認證登錄電腦執行該加密認證程式以該私鑰將該隨機字串加密而成。

【第3項】 如請求項1之登錄認證方法，其中在所述輸出隨機字串與網址的步驟中，所述使用者在該認證登錄電腦執行一加密認證程式，所述服務提供者電腦傳輸一二維條碼的數位影像至該加密認證程式，該二維條碼的資訊包含所述的隨機字串與所述的回傳簽章網址，該加密認證程式辨識該二維條碼的數位影像取得該服務提供者電腦給予的該隨機字串與該回傳簽章網址；所述接收數

位簽章的步驟中，該數位簽章是該認證登錄電腦執行該加密認證程式以該私鑰將該隨機字串加密而成。

【第4項】 如請求項1之登錄認證方法，其中在所述輸出隨機字串與網址的步驟中，所述服務提供者電腦在所述登錄電腦的一顯示器上顯示所述的隨機字串與所述的回傳簽章網址，所述使用者在該認證登錄電腦執行一加密認證程式並將該隨機字串與該回傳簽章網址輸入該加密認證程式，借此取得該服務提供者電腦給予的該隨機字串與該回傳簽章網址；所述接收數位簽章的步驟中，該數位簽章是該認證登錄電腦執行該加密認證程式以該私鑰將該隨機字串加密而成。

【第5項】 如請求項1之登錄認證方法，其中在所述輸出隨機字串與網址的步驟中，所述服務提供者電腦在所述登錄電腦的一顯示器上顯示提供所述使用者輸入的一手機號碼欄位或一電子信箱欄位；當所述認證登錄電腦是手機並且該使用者將手機號碼輸入該手機號碼欄位後，所述服務提供者電腦以簡訊將所述的隨機字串與所述的回傳簽章網址寄給該認證登錄電腦，使該認證登錄電腦取得該服務提供者電腦給予的該隨機字串與該回傳簽章網址；以及

當使用者將該認證登錄電腦能接收的電子信箱輸入該電子信箱欄位後，該服務提供者電腦以電子郵件將所述的隨機字串與所述的回傳簽章網址寄給該認證登錄電腦，使該認證登錄電腦取得該服務提供者電腦給予的該隨機字串與該回傳簽章網址；在所述接收數位簽章的步驟中，該數位簽章是該認證登錄電腦執行一加密認證程式以該私鑰將該隨機字串加密而成。

【第6項】 如請求項1之登錄認證方法，其中在所述輸出隨機字串與網址的步驟中，所述服務提供者電腦在所述登錄電腦的一顯示器上顯示提供所述使用者輸入的一認證服務網址欄位；所述認證登錄電腦是伺服器並且執行一加密認證程式提供網路上的認證服務，當使用者將該認證服務的認證服務網址輸入該

認證服務網址欄位後，該服務提供者電腦以查詢字串的方式將所述的隨機字串與所述的回傳簽章網址重導到認證服務網址，使該認證登錄電腦由該認證服務網址取得該服務提供者電腦給予的該隨機字串與該回傳簽章網址；所述接收數位簽章的步驟中，該數位簽章是該認證登錄電腦執行該加密認證程式以該私鑰將該隨機字串加密而成。

【第7項】 一種登錄認證方法，其步驟包括：

接收隨機字串與網址：與一金鑰驗證碼對應的成對私鑰與公鑰分別儲存在一認證登錄電腦以及一服務提供者電腦，該認證登錄電腦的使用者是該服務提供者電腦提供的一服務的使用者，當該使用者欲於一登錄電腦登錄該服務時，該服務提供者電腦依該使用者的要求給予一回傳簽章網址以及一隨機字串，該認證登錄電腦接收該回傳簽章網址以及該隨機字串；

輸出數位簽章：該認證登錄電腦以該私鑰將該隨機字串加密為一數位簽章，由該數位簽章能辨識出將其加密的該私鑰的金鑰驗證碼，將該數位簽章輸出至該回傳簽章網址；以及

被認證登錄：該數位簽章被該服務提供者電腦由該回傳簽章網址取得並以對應該金鑰驗證碼的該公鑰解開，若驗證該數位簽章內的該隨機字串與該服務提供者電腦給予使用者的該隨機字串相同，則允許該使用者在該登錄電腦登錄該服務。

【第8項】 如請求項7之登錄認證方法，其中在所述接收隨機字串與網址的步驟中，所述服務提供者電腦在所述登錄電腦的一顯示器上顯示一二維條碼，該二維條碼的資訊包含所述的隨機字串與所述的回傳簽章網址，所述使用者在該認證登錄電腦執行一加密認證程式，利用該認證登錄電腦的一鏡頭拍攝、辨識該二維條碼取得該服務提供者電腦給予的該隨機字串與該回傳簽章網址；所

述輸出數位簽章的步驟中，該數位簽章是該認證登錄電腦執行該加密認證程式以該私鑰將該隨機字串加密而成。

【第9項】 如請求項7之登錄認證方法，其中在所述接收隨機字串與網址的步驟中，所述使用者在該認證登錄電腦執行一加密認證程式，所述服務提供者電腦傳輸一二維條碼的數位影像至該加密認證程式，該二維條碼的資訊包含所述的隨機字串與所述的回傳簽章網址，該加密認證程式辨識該二維條碼的數位影像取得該服務提供者電腦給予的該隨機字串與該回傳簽章網址；所述輸出數位簽章的步驟中，該數位簽章是該認證登錄電腦執行該加密認證程式以該私鑰將該隨機字串加密而成。

【第10項】 如請求項7之登錄認證方法，其中在所述接收隨機字串與網址的步驟中，所述服務提供者電腦在所述登錄電腦的一顯示器上顯示所述的隨機字串與所述的回傳簽章網址，所述使用者在該認證登錄電腦執行一加密認證程式並將該隨機字串與該回傳簽章網址輸入該加密認證程式，借此取得該服務提供者電腦給予的該隨機字串與該回傳簽章網址；所述輸出數位簽章的步驟中，該數位簽章是該認證登錄電腦執行該加密認證程式以該私鑰將該隨機字串加密而成。

【第11項】 如請求項7之登錄認證方法，其中在所述接收隨機字串與網址的步驟中，所述服務提供者電腦在所述登錄電腦的一顯示器上顯示提供所述使用者輸入的一手機號碼欄位或一電子信箱欄位；當所述認證登錄電腦是手機並且該使用者將手機號碼輸入該手機號碼欄位後，所述服務提供者電腦以簡訊將所述的隨機字串與所述的回傳簽章網址寄給該認證登錄電腦，使該認證登錄電腦取得該服務提供者電腦給予的該隨機字串與該回傳簽章網址；以及

當使用者將該認證登錄電腦能接收的電子信箱輸入該電子信箱欄位後，該服務提供者電腦以電子郵件將所述的隨機字串與所述的回傳簽章網址寄給該認

證登錄電腦，使該認證登錄電腦取得該服務提供者電腦給予的該隨機字串與該回傳簽章網址；在所述輸出數位簽章的步驟中，該數位簽章是該認證登錄電腦執行一加密認證程式以該私鑰將該隨機字串加密而成。

【第12項】　如請求項7之登錄認證方法，其中在所述接收隨機字串與網址的步驟中，所述服務提供者電腦在所述登錄電腦的一顯示器上顯示提供所述使用者輸入的一認證服務網址欄位；所述認證登錄電腦是伺服器並且執行一加密認證程式提供網路上的認證服務，當使用者將該認證服務的認證服務網址輸入該認證服務網址欄位後，該服務提供者電腦以查詢字串的方式將所述的隨機字串與所述的回傳簽章網址重導到認證服務網址，使該認證登錄電腦由該認證服務網址取得該服務提供者電腦給予的該隨機字串與該回傳簽章網址；所述輸出數位簽章的步驟中，該數位簽章是該認證登錄電腦執行該加密認證程式以該私鑰將該隨機字串加密而成。

【發明圖式】

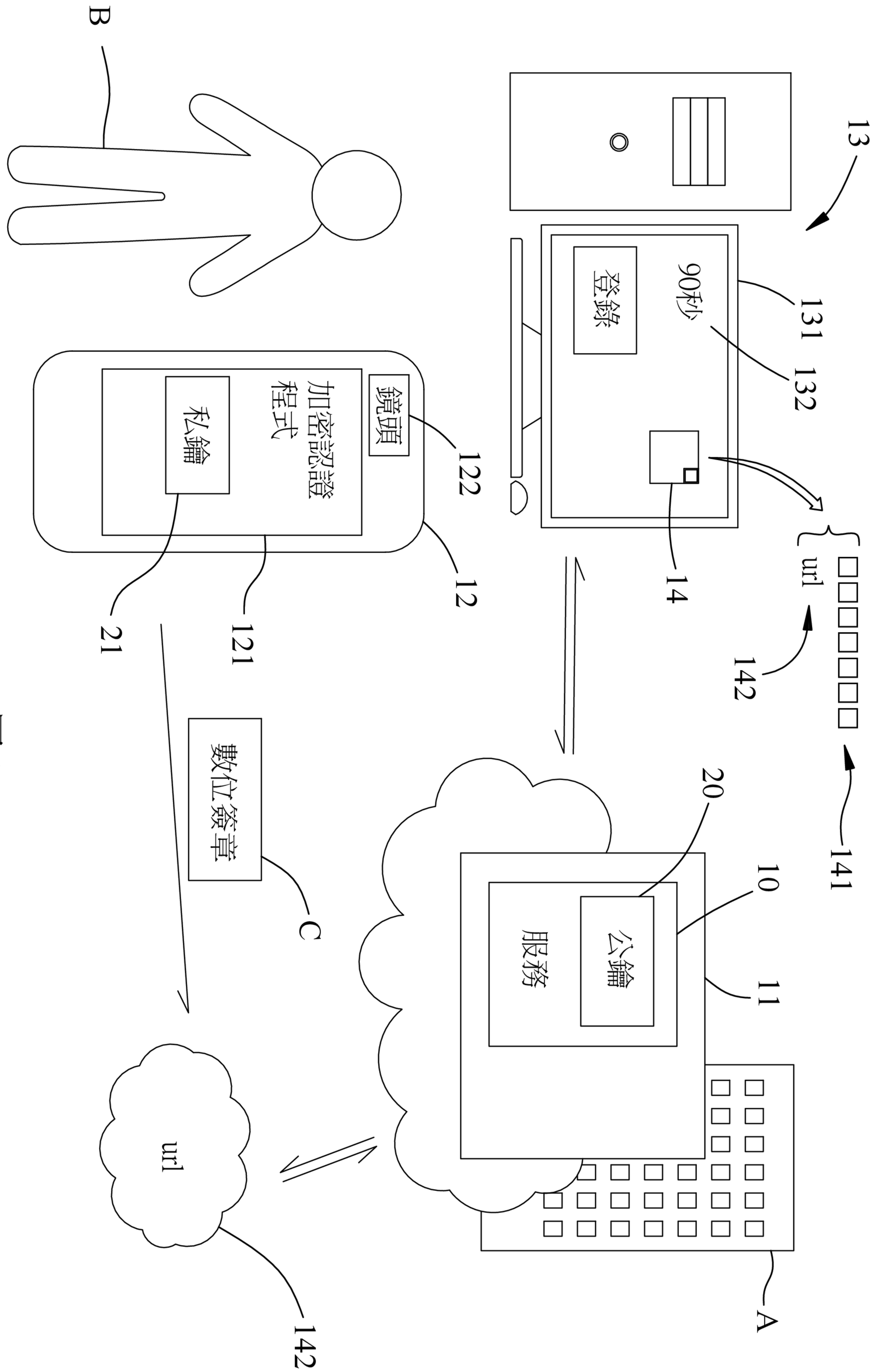

B
13
131
132
90秒
登錄
14
url
142
□□□□□□□□□□
141
122
鏡頭
加密認證程式
私鑰
12
21
121
數位簽章
C
20
10
11
公鑰
服務
url
142
A

圖 1

202037111

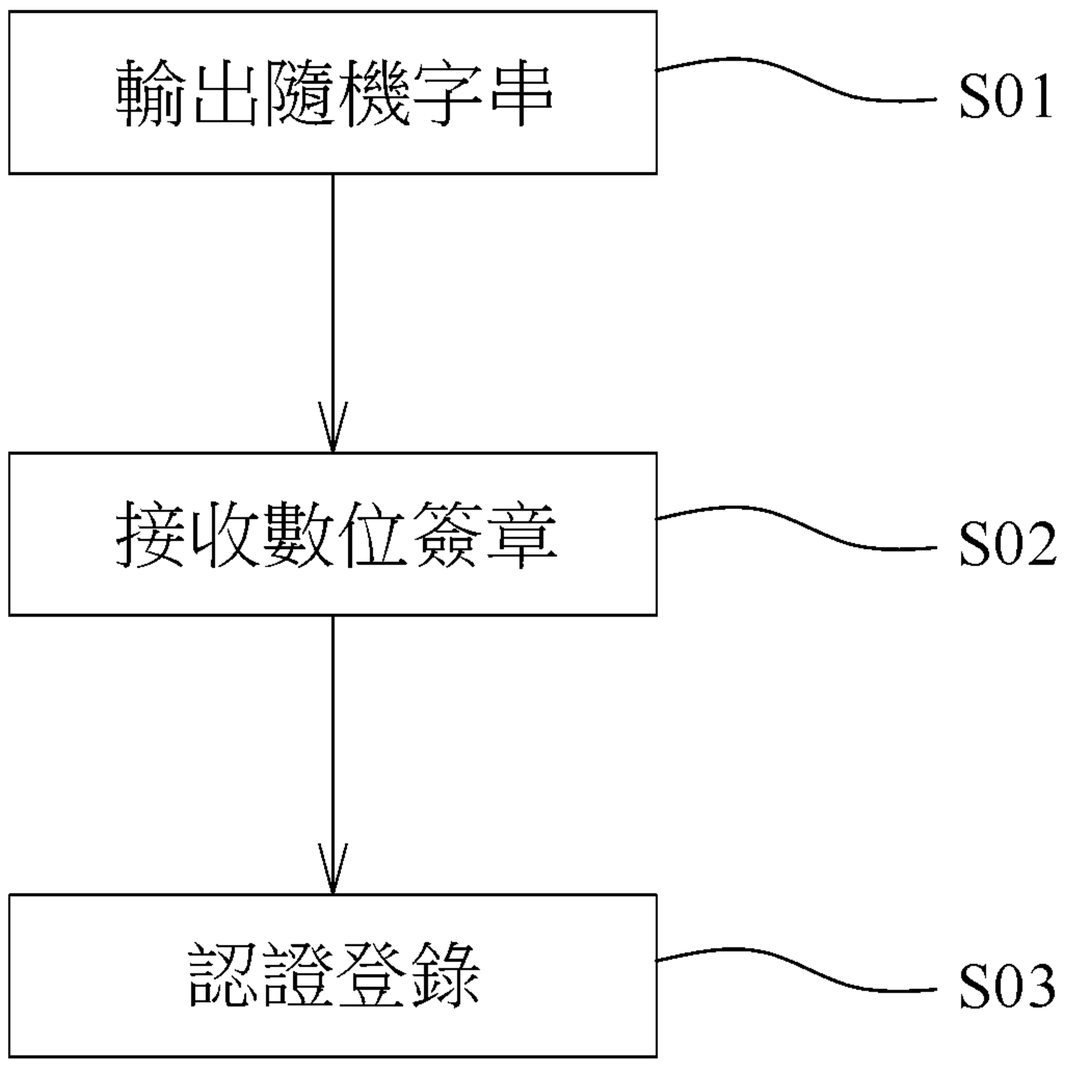


圖 2

202037111

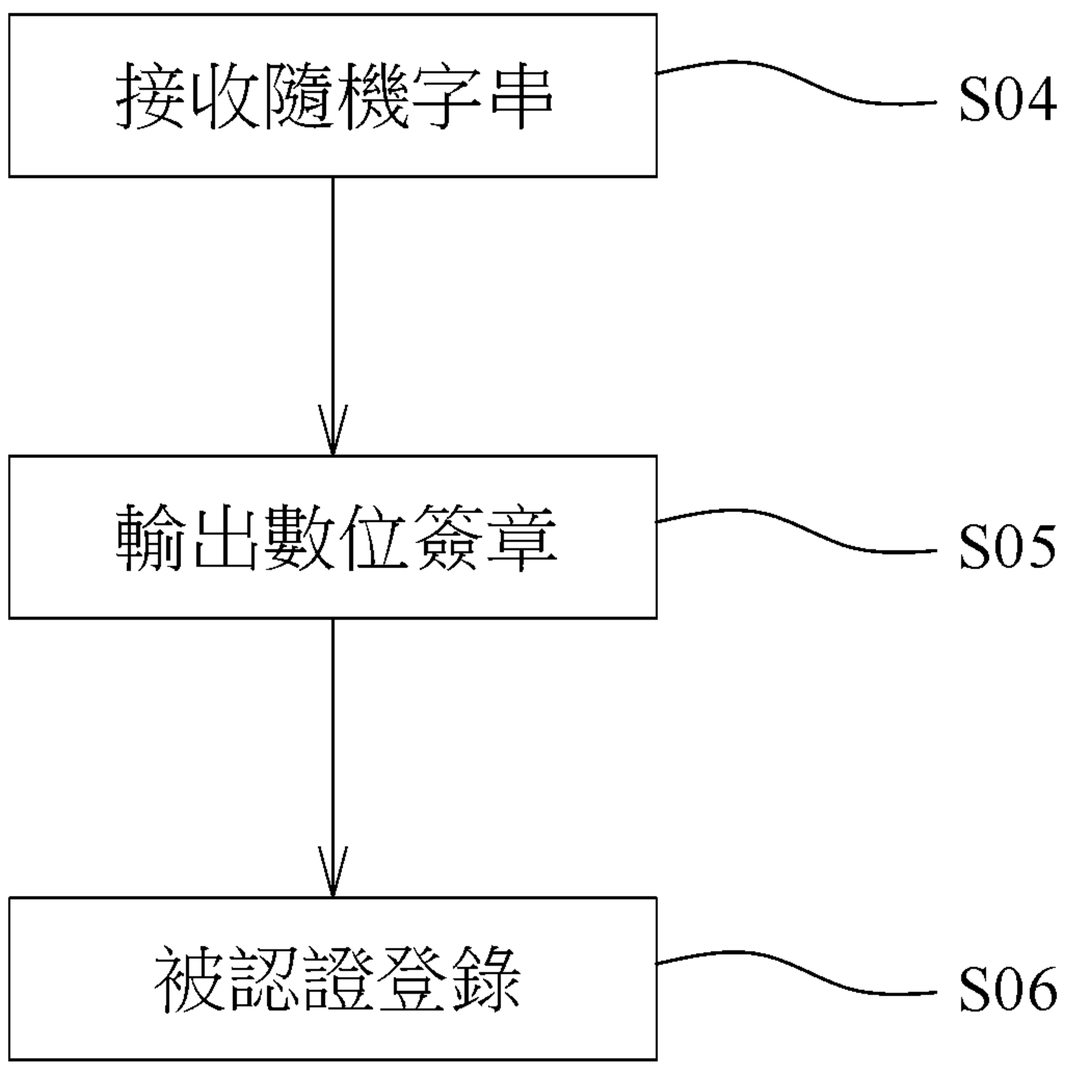


圖 3

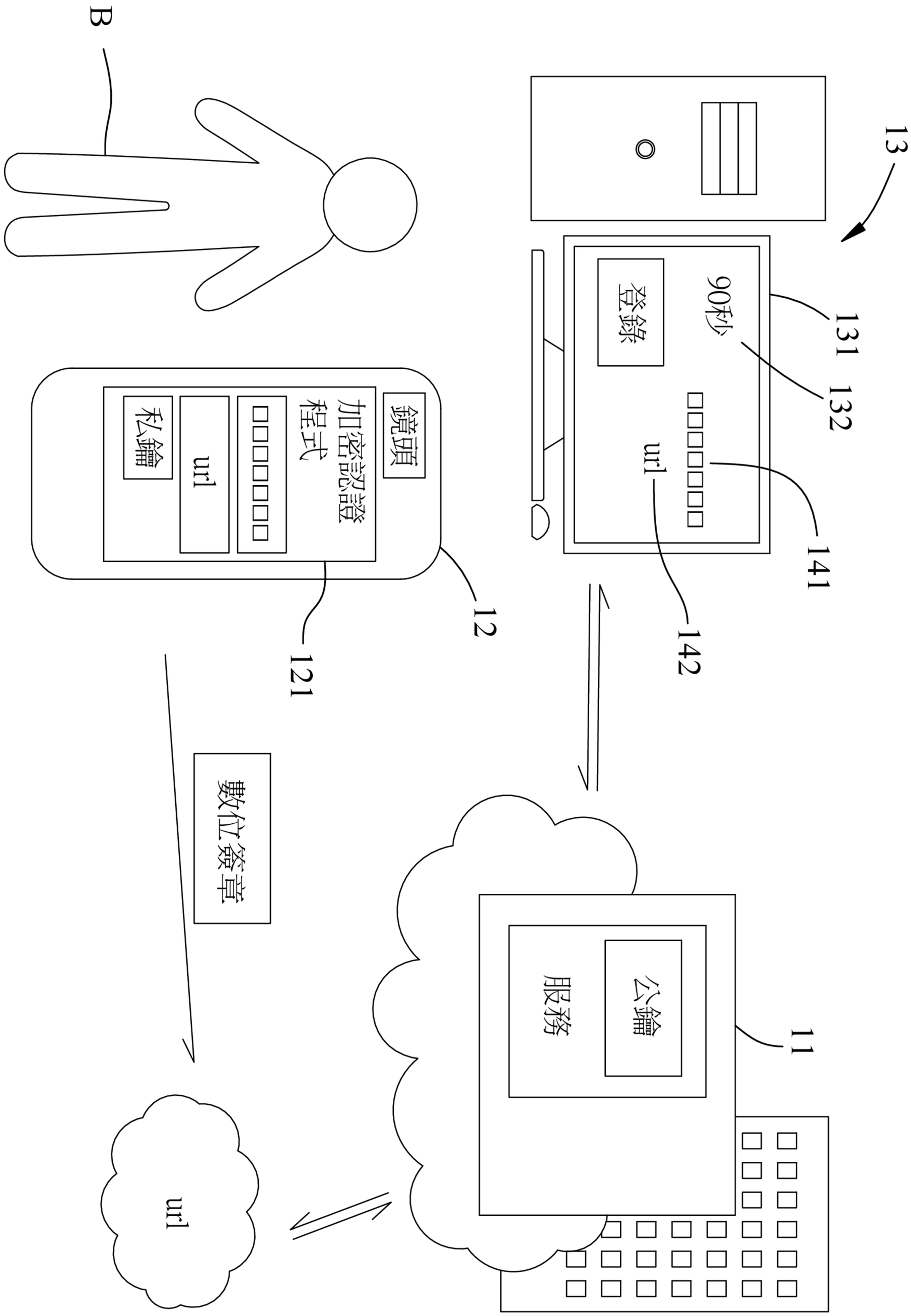

B
13
131
132
90秒
□□□□□□
登錄
url
141
142
鏡頭
加密認證程式
□□□□□□
url
私鑰
12
121
數位簽章
公鑰
服務
11
url

圖 4

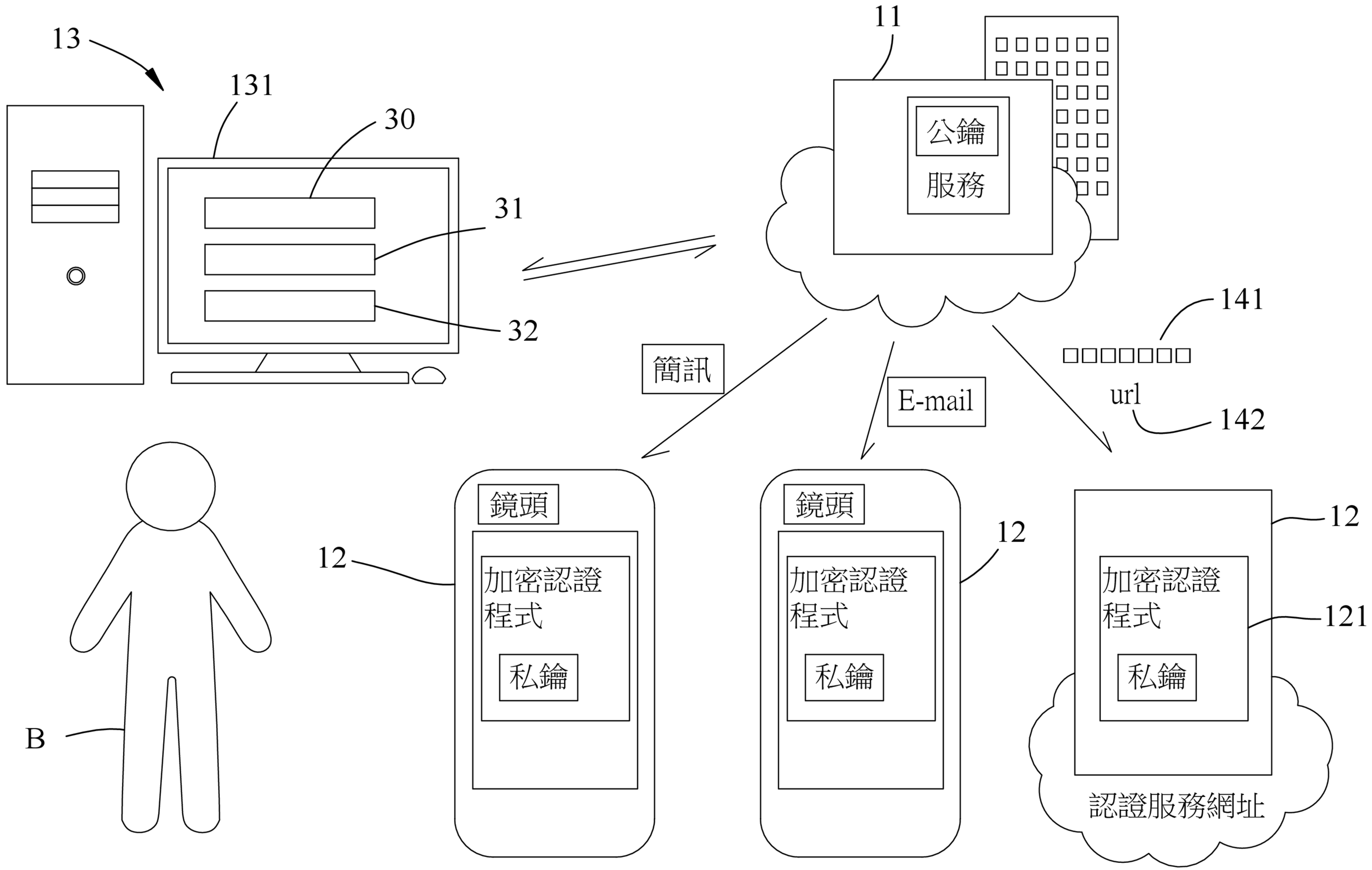

13
131
30
31
32
11
公鑰
服務
141
□□□□□□□
url
142
簡訊
E-mail
B
12
鏡頭
加密認證
程式
私鑰
12
鏡頭
加密認證
程式
私鑰
12
121
加密認證
程式
私鑰
認證服務網址

圖 5

108年5月1日 所提修正

申請日：

IPC 分類：

【發明摘要】

【中文發明名稱】 登錄認證方法

【英文發明名稱】 Login authentication method

【中文】

一種登錄認證方法，與一金鑰驗證碼對應的成對公、私鑰分別儲存在服務提供者與使用者的電腦後，當該使用者欲在一登錄電腦登錄該服務時，服務提供者給予該使用者一隨機字串與一回傳簽章網址儲存至使用者的電腦，該使用者的電腦以私鑰將該隨機字串加密為一數位簽章後，傳輸至該回傳簽章網址供服務提供者電腦取得，服務提供者電腦以該公鑰解密驗證該隨機字串是否正確，若正確則令該使用者登錄該服務；藉由上述登錄認證的方法，使得使用者登錄服務時不需要背誦帳號與密碼，不會有遺失帳號密碼的問題，登錄的程序簡便且具有較高的安全性。

【英文】

A login authentication method provides a key verification code and a corresponding pair of public key and private key being respectively stored in the service provider and an user's computer. When the user login to the service, the service provider gives a random string and a returning signature URL to the user's computer. The user's computer encrypts the random string into a digital signature with a private key, and transmits it to the return signature website for the service provider computer. The service provider computer decrypts with the public key to verify that the random string is correct, and if correct, the user is logged into the service. By the above method, users may login to the service without reciting their account and password. There will

be no problem with losing the account and password and the login procedure is simple and highly secure.

【指定代表圖】 圖1

【代表圖之符號簡單說明】

10服務

11服務提供者電腦

12認證登錄電腦

121加密認證程式

122鏡頭

13登錄電腦

131顯示器

132登錄時限

14二維條碼

141隨機字串

142回傳簽章網址

20公鑰

21私鑰

A服務提供者

B使用者

C數位簽章

【發明說明書】

【中文發明名稱】 登錄認證方法

【英文發明名稱】 Login authentication method

【技術領域】

【0001】 本發明涉及一種非對稱金鑰的認證方法，尤其涉及一種登錄時取得字串加密為簽章登錄的登錄認證方法。

【先前技術】

【0002】 現有的網路服務，例如電子郵件、社群網站或者即時通訊軟體在登錄服務時，主要是以註冊服務時所得到的帳號與密碼在個人電腦或手機登錄上述的網路服務，帳號通常是設定為使用者的電子郵件信箱，在使用者註冊後服務提供者將對應帳號的密碼寄往使用者的電子郵件信箱，供使用者接收並在序登錄服務時使用。

【0003】 由於上述登錄網路服務的方式是以帳號、密碼的方式登錄服務，因此使用者需要在程式或網頁的介面中輸入帳號、密碼才能登錄服務，甚至有些人因為擔心遺忘帳號密碼而將帳號密碼寫在手札或筆記上，如此需要背誦帳號密碼的方式，除了使得登錄服務的過程較為麻煩以外，帳號密碼寫在札記或筆記上也容易被盜取而產生資訊安全上的問題。

【發明內容】

【0004】 由於現有登錄網路服務的方式需要使用帳號密碼，除了容易遺忘以外也容易被盜取造成安全性問題。為此，本發明利用成對的金鑰配合隨機字串的加解密，能夠達到安全且無需輸入帳號密碼的認證登錄效果。

【0005】 為達到上述目的，本發明提供一種服務提供者電腦端的登錄認證方法，其步驟包括：

【0006】 輸出隨機字串與網址：與一金鑰驗證碼對應的成對私鑰與公鑰分別儲存在一認證登錄電腦以及一服務提供者電腦，該服務提供者電腦提供一服務，該使用者欲於一登錄電腦登錄該服務時，該服務提供者電腦依該使用者要求給予一回傳簽章網址以及一隨機字串；

【0007】 接收數位簽章：該服務提供者電腦由該回傳簽章網址接收該認證登錄電腦回傳的一數位簽章，該數位簽章是該認證登錄電腦以該私鑰將該隨機字串加密而成，由該數位簽章能辨識出將其加密的該私鑰的金鑰驗證碼；以及

【0008】 認證登錄：該服務提供者電腦以對應該金鑰驗證碼的該公鑰解開該數位簽章，驗證該數位簽章內的該隨機字串與該服務提供者電腦給予使用者的該隨機字串是否相同，若相同則允許該使用者在該登錄電腦登錄該服務。

【0009】 較佳的，本發明在所述輸出隨機字串與網址的步驟中，所述服務提供者電腦在所述登錄電腦的一顯示器上顯示一二維條碼，該二維條碼的資訊包含所述的隨機字串與所述的回傳簽章網址，所述使用者在該認證登錄電腦執行一加密認證程式，利用該認證登錄電腦的一鏡頭拍攝、辨識該二維條碼取得該服務提供者電腦給予的該隨機字串與該回傳簽章網址；所述接收數位簽章的步驟中，該數位簽章是該認證登錄電腦執行該加密認證程式以該私鑰將該隨機字串加密而成。

【0010】 較佳的，本發明在所述輸出隨機字串與網址的步驟中，所述服務提供者電腦在所述登錄電腦的一顯示器上顯示所述的隨機字串與所述的回傳簽章網址，所述使用者在該認證登錄電腦執行一加密認證程式並將該隨機字串與該回傳簽章網址輸入該加密認證程式，借此取得該服務提供者電腦給予的該隨

機字串與該回傳簽章網址；所述接收數位簽章的步驟中，該數位簽章是該認證登錄電腦執行該加密認證程式以該私鑰將該隨機字串加密而成。

【0011】 較佳的，本發明在所述輸出隨機字串與網址的步驟中，所述服務提供者電腦在所述登錄電腦的一顯示器上顯示提供所述使用者輸入的一手機號碼欄位或一電子信箱欄位；當所述認證登錄電腦是手機並且該使用者將手機號碼輸入該手機號碼欄位後，所述服務提供者電腦以簡訊將所述的隨機字串與所述的回傳簽章網址寄給該認證登錄電腦，使該認證登錄電腦取得該服務提供者電腦給予的該隨機字串與該回傳簽章網址；以及當使用者將該認證登錄電腦能接收的電子信箱輸入該電子信箱欄位後，該服務提供者電腦以電子郵件將所述的隨機字串與所述的回傳簽章網址寄給該認證登錄電腦，使該認證登錄電腦取得該服務提供者電腦給予的該隨機字串與該回傳簽章網址；在所述接收數位簽章的步驟中，該數位簽章是該認證登錄電腦執行一加密認證程式以該私鑰將該隨機字串加密而成。

【0012】 較佳的，本發明在所述輸出隨機字串與網址的步驟中，所述服務提供者電腦在所述登錄電腦的一顯示器上顯示提供所述使用者輸入的一認證服務網址欄位；所述認證登錄電腦是伺服器並且執行一加密認證程式提供網路上的認證服務，當使用者將該認證服務的認證服務網址輸入該認證服務網址欄位後，該服務提供者電腦以查詢字串的方式將所述的隨機字串與所述的回傳簽章網址重導到認證服務網址，使該認證登錄電腦由該認證服務網址取得該服務提供者電腦給予的該隨機字串與該回傳簽章網址；所述接收數位簽章的步驟中，該數位簽章是該認證登錄電腦執行該加密認證程式以該私鑰將該隨機字串加密而成。

【0013】 本發明又提供一種認證登錄電腦端的登錄認證方法，其步驟包括：

【0014】 接收隨機字串與網址：與一金鑰驗證碼對應的成對私鑰與公鑰分別儲存在一認證登錄電腦以及一服務提供者電腦，該認證登錄電腦的使用者是該服務提供者電腦提供的一服務的使用者，當該使用者欲於一登錄電腦登錄該服務時，該服務提供者電腦依該使用者的要求給予一回傳簽章網址以及一隨機字串，該認證登錄電腦接收該回傳簽章網址以及該隨機字串；

【0015】 輸出數位簽章：該認證登錄電腦以該私鑰將該隨機字串加密為一數位簽章，由該數位簽章能辨識出將其加密的該私鑰的金鑰驗證碼，將該數位簽章輸出至該回傳簽章網址；以及

【0016】 被認證登錄：該數位簽章被該服務提供者電腦由該回傳簽章網址取得並以對應該金鑰驗證碼的該公鑰解開，若驗證該數位簽章內的該隨機字串與該服務提供者電腦給予使用者的該隨機字串相同，則允許該使用者在該登錄電腦登錄該服務。

【0017】 較佳的，本發明在所述接收隨機字串與網址的步驟中，所述服務提供者電腦在所述登錄電腦的一顯示器上顯示一二維條碼，該二維條碼的資訊包含所述的隨機字串與所述的回傳簽章網址，所述使用者在該認證登錄電腦執行一加密認證程式，利用該認證登錄電腦的一鏡頭拍攝、辨識該二維條碼取得該服務提供者電腦給予的該隨機字串與該回傳簽章網址；所述輸出數位簽章的步驟中，該數位簽章是該認證登錄電腦執行該加密認證程式以該私鑰將該隨機字串加密而成。

【0018】 較佳的，本發明在所述接收隨機字串與網址的步驟中，所述服務提供者電腦在所述登錄電腦的一顯示器上顯示所述的隨機字串與所述的回傳簽章網址，所述使用者在該認證登錄電腦執行一加密認證程式並將該隨機字串與該回傳簽章網址輸入該加密認證程式，借此取得該服務提供者電腦給予的該隨

機字串與該回傳簽章網址；所述輸出數位簽章的步驟中，該數位簽章是該認證登錄電腦執行該加密認證程式以該私鑰將該隨機字串加密而成。

【0019】 較佳的，本發明在所述接收隨機字串與網址的步驟中，所述服務提供者電腦在所述登錄電腦的一顯示器上顯示提供所述使用者輸入的一手機號碼欄位或一電子信箱欄位；當所述認證登錄電腦是手機並且該使用者將手機號碼輸入該手機號碼欄位後，所述服務提供者電腦以簡訊將所述的隨機字串與所述的回傳簽章網址寄給該認證登錄電腦，使該認證登錄電腦取得該服務提供者電腦給予的該隨機字串與該回傳簽章網址；以及當使用者將該認證登錄電腦能接收的電子信箱輸入該電子信箱欄位後，該服務提供者電腦以電子郵件將所述的隨機字串與所述的回傳簽章網址寄給該認證登錄電腦，使該認證登錄電腦取得該服務提供者電腦給予的該隨機字串與該回傳簽章網址；在所述輸出數位簽章的步驟中，該數位簽章是該認證登錄電腦執行一加密認證程式以該私鑰將該隨機字串加密而成。

【0020】 較佳的，本發明在所述接收隨機字串與網址的步驟中，所述服務提供者電腦在所述登錄電腦的一顯示器上顯示提供所述使用者輸入的一認證服務網址欄位；所述認證登錄電腦是伺服器並且執行一加密認證程式提供網路上的認證服務，當使用者將該認證服務的認證服務網址輸入該認證服務網址欄位後，該服務提供者電腦以查詢字串的方式將所述的隨機字串與所述的回傳簽章網址重導到認證服務網址，使該認證登錄電腦由該認證服務網址取得該服務提供者電腦給予的該隨機字串與該回傳簽章網址；所述輸出數位簽章的步驟中，該數位簽章是該認證登錄電腦執行該加密認證程式以該私鑰將該隨機字串加密而成。

【0021】 本發明的功效在於，透過本發明的方法能讓服務提供者電腦給予認證登錄電腦隨機字串與回傳簽章網址，利用私鑰加密隨機字串為數位簽章

後，回傳至該回傳簽章網址供服務提供者電腦取得並進行使用者的身份驗證，過程加密且能在當下由隨機字串的比對，確認請求登錄服務者是否是對應金鑰驗證碼的該服務的使用者，讓使用者無需在登錄電腦輸入帳號、密碼，即可由成對的公鑰、私鑰加解密該隨機字串的方式，讓使用者在任一登錄電腦上登錄該服務，避免背誦帳號、密碼的不便以及帳號、密碼容易遺失可能造成的安全性問題。

【圖式簡單說明】

【0022】

圖1是本發明第一較佳實施例方法的示意圖。

圖2是本發明第一較佳實施例該服務提供者端的流程圖。

圖3是本發明第一較佳實施例該使用者端的流程圖。

圖4是本發明第二較佳實施例方法的示意圖。

圖5是本發明第三較佳實施例方法的示意圖。

【實施方式】

【0023】 為能詳細瞭解本發明的技術特徵及實用功效，並可依照說明書的內容來實施，進一步以如圖式所示的較佳實施例，詳細說明如下。

【0024】 請參看如圖1至圖3所示的本發明第一較佳實施例，是提供一種登錄認證方法，用以登錄一服務提供者A提供的網路的服務10，例如電子郵件、社群網站、即時通訊軟體、購物網站、集資網站或網路論壇的服務。

【0025】 上述的服務10是架設在一服務提供者電腦11，例如伺服器或雲端的虛擬伺服器，當一使用者B註冊該服務時是先以一認證登錄電腦12例如手機或平板，以該認證登錄電腦12網路瀏覽器執行的加解密程式，或預先安裝在該認

證登錄電腦12的一加密認證程式121連上該服務10進行帳號的註冊，在註冊過程中產生與一金鑰驗證碼(Key ID)對應且成對的公鑰20與私鑰21，其中公鑰20儲存在該服務提供者電腦11，該服務提供者A能以該金鑰驗證碼辨識該使用者B的身分以及對應該使用者B的公鑰20，該私鑰21則儲存在該認證登錄電腦12而能供該加密認證程式121使用。

【0026】 如圖1至圖2所示，在使用者B註冊該服務10之後，本較佳實施例的該服務提供者A接受使用者B登錄該服務10的步驟S01至步驟S03包括：

【0027】 （S01）輸出隨機字串與網址：與一金鑰驗證碼(Key ID)對應的成對私鑰21與公鑰20已分別儲存在該認證登錄電腦12以及該服務提供者電腦11，該服務提供者電腦11提供一網路的服務10，該認證登錄電腦12執行一加密認證程式121。

【0028】 當使用者B要在某一登錄電腦13透過網路登錄該服務10時，該服務提供者電腦11依使用者B在該登錄電腦13上的要求，例如在該登錄電腦13的網路瀏覽器登錄該服務10時觸發登錄的要求，使得該服務提供者電腦11在一登錄時限132，例如90秒內於該登錄電腦13的顯示器131上顯示一二維條碼14，例如QR Code，該二維條碼14的資訊包含一隨機字串141與一回傳簽章網址142，每次登錄時限132內或分別刷新登錄網頁時產生在該顯示器131的二維條碼14所包含的隨機字串141不同。接著使用者B執行該加密認證程式121，利用該認證登錄電腦12的鏡頭122拍攝該二維條碼14，辨識後自動取得該服務提供者電腦11給予的該隨機字串141與該回傳簽章網址142。

【0029】 （S02）接收數位簽章：該服務提供者電腦11由網路接收該認證登錄電腦12回傳至該回傳簽章網址142的一數位簽章C，該數位簽章C是該認證登錄電腦12執行該加密認證程式121以該私鑰21加密該隨機字串141而成，由該數位簽章C能辨識出將其加密的該私鑰的金鑰驗證碼。

【0030】 （S03）認證登錄：該服務提供者電腦11以對應該金鑰驗證碼的該公鑰20解開該數位簽章C，驗證該數位簽章C內的該隨機字串141與該服務提供者電腦11當次的登錄時限132所輸出的該隨機字串141是否相同，若相同則允許該使用者B在該登錄電腦13登錄該服務10，若不同則拒絕該使用者B在該登錄電腦13登錄該服務10。

【0031】 如圖1、圖3所示，在使用者B註冊該服務10之後，該使用者B登錄該服務10的步驟S04至步驟S06包括：

【0032】 （S04）接收隨機字串與網址：與一金鑰驗證碼(Key ID)對應的成對私鑰21與公鑰20已分別儲存在該認證登錄電腦12以及該服務提供者電腦11，該使用者B為該服務提供者電腦11提供的一網路的服務10的使用者，且該認證登錄電腦12已安裝一加密認證程式121；該服務提供者電腦11依使用者B在某一登錄電腦13發出的登錄該服務10的要求，在一登錄時限132例如90秒內，於該登錄電腦13的顯示器131上顯示一二維條碼14，例如 QR Code，該二維條碼14的資訊包含一隨機字串141與一回傳簽章網址142，每次登錄時限132或刷新登錄網頁時所產生的隨機字串141會逐次更新；使用者B透過執行該加密認證程式121驅動該認證登錄電腦12的鏡頭122拍攝辨識該二維條碼14，辨識後獲得該服務提供者電腦11給予的該隨機字串141與該回傳簽章網址142。

【0033】 （S05）輸出數位簽章：該認證登錄電腦12執行的該加密認證程式121在取得該隨機字串141後，以該私鑰21將該隨機字串141加密為一數位簽章C，由該數位簽章C能辨識出將其加密的該私鑰的金鑰驗證碼，透過網路將該數位簽章C輸出至該回傳簽章網址142，供該服務提供者電腦11取得。

【0034】 （S06）被認證登錄：該數位簽章C被該服務提供者電腦11以對應該金鑰驗證碼的該公鑰20解開，驗證該數位簽章C內的該隨機字串141與該服務提供者電腦11當次的登錄時限132所輸出的該隨機字串141是否相同，若相同

則允許該使用者B在該登錄電腦13登錄該服務10，若不同則拒絕該使用者B在該登錄電腦13登錄該服務10。

【0035】 本發明除前述第一較佳實施例，在進行該輸出隨機字串與網址的步驟（S01）或該接收隨機字串與網址的步驟（S04）時，是以該認證登錄電腦12的鏡頭122拍攝該二維條碼14，辨識後取得該服務提供者電腦11給予的該隨機字串141與該回傳簽章網址142以外，該服務提供者電腦11於該登錄電腦13的顯示器131上顯示的二維條碼14，也能透過網路硬碟、藍牙傳輸、SD卡轉存等手段，將該二維條碼14的數位影像傳輸給該認證登錄電腦12的該加密認證程式121讀取，使該加密認證程式121辨識該二維條碼14的數位影像後，取得該服務提供者電腦11給予的該隨機字串141與該回傳簽章網址14。或者如以下所述的第二較佳實施例或第三較佳實施例，依使用者B的要求，該服務提供者電腦11可透過其他手段給予該隨機字串141與該回傳簽章網址142。

【0036】 如圖4所示的第二較佳實施例，該服務提供者電腦11依使用者B在該登錄電腦13上的要求，在所述的登錄時限132內於該登錄電腦13的顯示器131上顯示所述的隨機字串141與所述的回傳簽章網址142，每次登錄時限132或刷新登錄網頁時所產生的隨機字串141會逐次更新；使用者B將該隨機字串141與該回傳簽章網址142輸入該加密認證程式121，使該認證登錄電腦12手動地取得該服務提供者電腦11給予的該隨機字串141與該回傳簽章網址142，提供該加密認證程式121在後續的步驟（S02）或步驟（S05）執行使用。

【0037】 如圖5所示的第三較佳實施例，該服務提供者電腦11依使用者B在該登錄電腦13上的要求，在該登錄電腦13的顯示器13上顯示提供使用者B輸入的手機號碼欄位30（若該認證登錄電腦12為手機）、電子信箱欄位31，或認證服務網址欄位32（若該認證登錄電腦12是伺服器，且執行所述加密認證程式121提供網路上的認證服務）。

【0038】 首先，當使用者B將該認證登錄電腦12（即手機）的手機號碼輸入該手機號碼欄位30後，該服務提供者電腦11以簡訊的方式將所述的隨機字串141與所述的回傳簽章網址142寄給該認證登錄電腦12，使該認證登錄電腦12自動地取得該服務提供者電腦11給予的該隨機字串141與該回傳簽章網址142，提供所述的加密認證程式121在後續的步驟（S02）或步驟（S05）執行使用。

【0039】 其次，當使用者B將該認證登錄電腦12能接收的電子信箱輸入該電子信箱欄位31後，該服務提供者電腦11以電子郵件的方式將所述的隨機字串141與所述的回傳簽章網址142寄給該認證登錄電腦12，使該認證登錄電腦12自動地取得該服務提供者電腦11給予的該隨機字串141與該回傳簽章網址142，提供所述的加密認證程式121在後續的步驟（S02）或步驟（S05）執行使用。

【0040】 再者，當使用者B將該認證登錄電腦12（即伺服器）執行該加密認證程式121的認證服務網址輸入該認證服務網址欄位32後，該服務提供者電腦11以查詢字串（QueryString）的方式將所述的隨機字串141與所述的回傳簽章網址142重導到認證服務網址，使該認證登錄電腦12由該認證服務網址自動地取得該服務提供者電腦11給予的該隨機字串141與該回傳簽章網址142，提供所述的加密認證程式121在後續的步驟（S02）或步驟（S05）執行使用。

【0041】 以上所述僅為本發明的較佳實施例而已，並非用以限定本發明主張的權利範圍，凡其它未脫離本發明所揭示的精神所完成的等效改變或修飾，均應包括在本發明的申請專利範圍內。

【符號說明】

【0042】

S01步驟 S02步驟

S03步驟 S04步驟

S05步驟

S06步驟

10服務

11服務提供者電腦

12認證登錄電腦

121加密認證程式

122鏡頭

13登錄電腦

131顯示器

132登錄時限

14二維條碼

141隨機字串

142回傳簽章網址

20公鑰

21私鑰

A服務提供者

B使用者

C數位簽章

30手機號碼欄位

31電子信箱欄位

32認證服務網址欄位