I727793

(19)中華民國智慧財產局

(12)發明說明書公告本　**(11)證書號數：TW I727793 B**

(45)公告日： 中華民國 110 (2021) 年 05 月 11 日

(21)申請案號：109115592　(22)申請日： 中華民國 109 (2020) 年 05 月 11 日

(51)Int. Cl.：　*H04L9/30　(2006.01)*　*G06F21/62　(2013.01)*

(30)優先權：2020/04/14　中國大陸　202010291921.3

(71)申請人：威盛電子股份有限公司 (中華民國) VIA TECHNOLOGIES, INC.　(TW)

新北市新店區中正路 533 號 8 樓

(72)發明人：徐耀忠 XU, YAOZHONG (CN)

(74)代理人：葉璟宗；卓俊傑

(56)參考文獻：

TW	I460662B	TW	M584934U
CN	107103255A	CN	109615038A
US	9418326B1	US	2016/0294821A1
US	2020/0092272A1		

審查人員：周官緯

申請專利範圍項數：34 項　圖式數：7　共 41 頁

(54)名稱

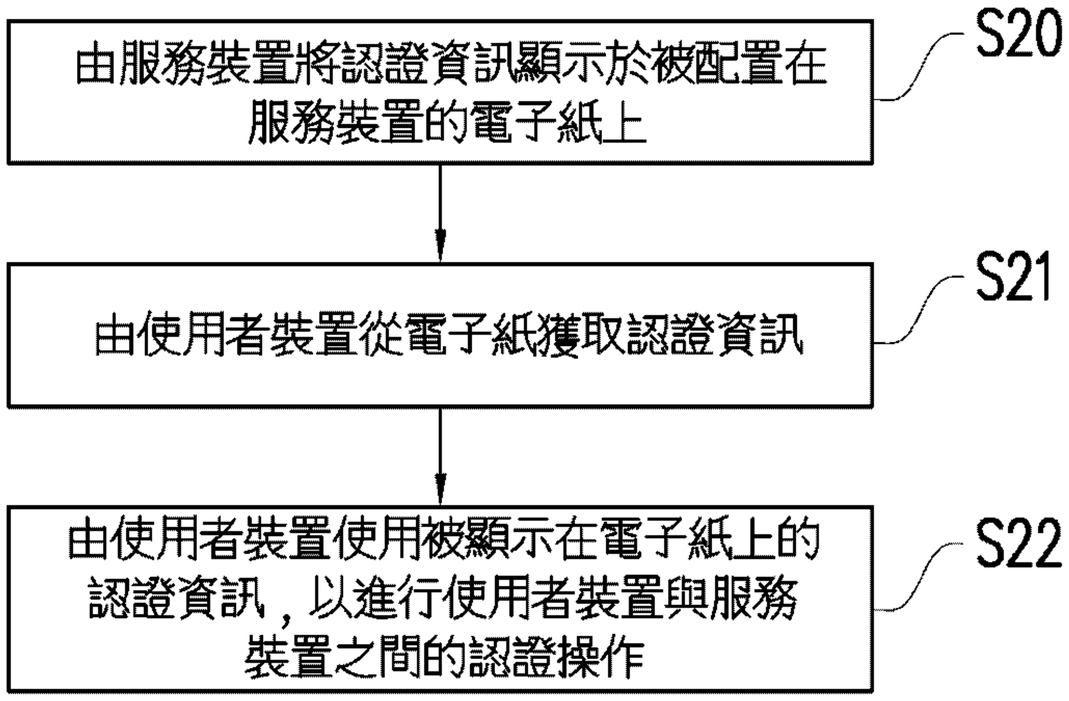
認證方法及認證系統

(57)摘要

本發明提供一種認證方法及認證系統。認證方法包含由服務裝置將認證資訊顯示於被配置在服務裝置的電子紙上；由使用者裝置從電子紙獲取認證資訊；以及由使用者裝置使用被顯示在電子紙上的認證資訊，以進行使用者裝置與服務裝置之間的認證操作。

An authorization method and an authorization system are provided. The authorization method includes displaying, by a service device, authorization information on an e-paper arranged on the service device; obtaining, by a user device, the authorization information from the e-paper; and using, by the user device, the authorization information displayed on the e-paper to perform an authorization operation between the user device and the service device.

指定代表圖：



【圖2】

符號簡單說明：

S20~S22:步驟

專利案號：109115592

公告本

I727793

【發明摘要】

【中文發明名稱】認證方法及認證系統

【英文發明名稱】AUTHORIZATION METHOD AND AUTHORIZATION SYSTEM

【中文】本發明提供一種認證方法及認證系統。認證方法包含由服務裝置將認證資訊顯示於被配置在服務裝置的電子紙上；由使用者裝置從電子紙獲取認證資訊；以及由使用者裝置使用被顯示在電子紙上的認證資訊，以進行使用者裝置與服務裝置之間的認證操作。

【英文】An authorization method and an authorization system are provided. The authorization method includes displaying, by a service device, authorization information on an e-paper arranged on the service device; obtaining, by a user device, the authorization information from the e-paper; and using, by the user device, the authorization information displayed on the e-paper to perform an authorization operation between the user device and the service device.

【指定代表圖】圖2。

【代表圖之符號簡單說明】

S20～S22：步驟

【特徵化學式】

無

【發明說明書】

【中文發明名稱】認證方法及認證系統

【英文發明名稱】AUTHORIZATION METHOD AND AUTHORIZATION SYSTEM

【技術領域】

【0001】 本發明是有關於一種方法及系統，且特別是有關於一種認證方法及認證系統。

【先前技術】

【0002】 習知無線網路設備（服務裝置）的出廠設置是使用固定的初始用戶名稱與固定的初始密碼。使用者裝置可以使用初始用戶名稱與初始密碼登入服務裝置，以設定/控制服務裝置。初始用戶名稱與初始密碼被記錄在某個地方，比如記錄在黏貼於設備上的貼紙，以及/或是記錄在設備的說明書上。大部分使用者不會修改初始用戶名稱與初始密碼，所以駭客很容易猜測（或者獲取）習知無線網路設備的初始用戶名稱與初始密碼。即便使用者修改用戶名稱與密碼，大部分人都選擇容易記憶的用戶名稱與密碼(甚至是多個設備使用同一個密碼)，而且也不會時常更新密碼。因此，習知無線網路設備的安全係數低（亦即易被入侵）。

【0003】 此外，在傳統的認證系統中，使用者裝置與服務裝置要利用相同的通訊網路傳遞（或是交換）公鑰（public key）以及進

行認證操作。當傳遞（或是交換）公鑰時，非法裝置可能會從所述通訊網路（電性網路，例如網際網路）攔截真公鑰，並以假公鑰取代真公鑰。因此，傳統的認證系統可能會有資安問題。

【0004】 再舉例而言，當服務裝置透過網路提供包含有密碼的認證資訊給使用者裝置時，認證資訊可能會透過網路封包被第三者竊取，造成密碼的外洩。或者，當使用者裝置欲連接至認證頁面來進行認證時，可能會連結至錯誤的釣魚網站，導致密碼的外洩。又或者，服務裝置中所儲存的帳號及密碼等資料，只要服務裝置遭到入侵就會造成密碼的外洩。因此，傳統的認證方法及認證系統存在著資訊安全的風險。

【發明內容】

【0005】 本發明提供一種認證方法及認證系統，其可以提昇資訊安全。

【0006】 本發明的認證方法包含由服務裝置將認證資訊顯示於被配置在服務裝置的電子紙上；由使用者裝置從電子紙獲取認證資訊；以及由使用者裝置使用被顯示在電子紙上的認證資訊，以進行使用者裝置與服務裝置之間的認證操作。

【0007】 本發明的認證系統包含服務裝置及使用者裝置。服務裝置包含電子紙以及處理器，其中處理器被配置為控制電子紙，以將認證資訊顯示於電子紙上。使用者裝置用來從電子紙獲取認證資訊，並且使用被顯示在電子紙上的認證資訊，以進行使用者裝

置與服務裝置之間的認證操作。

【0008】 基於上述，本發明實施例所述的認證方法及認證系統可以透過服務裝置上的電子紙來傳遞認證資訊。使用者裝置使用顯示在電子紙的認證資訊來進行使用者裝置與服務裝置之間的認證操作。如此一來，服務裝置所提供的認證資訊可以避免在通訊網路中傳遞（避免非法裝置從通訊網路截取認證資訊），進而有效改善認證方法及認證系統的資訊安全。

【圖式簡單說明】

【0009】

圖 1 為本發明實施例一認證系統的電路方塊（circuit block）示意圖。

圖 2 為本發明實施例一認證方法的流程示意圖。

圖 3 為本發明另一實施例的一認證方法的流程示意圖。

圖 4 為本發明另一實施例的一認證方法的流程示意圖。

圖 5 為本發明另一實施例的一認證方法的流程示意圖。

圖 6 為本發明另一實施例的一認證方法的流程示意圖。

圖 7 為本發明另一實施例的一認證方法的流程示意圖。

【實施方式】

【0010】 請參考圖 1，圖 1 為本發明實施例一認證系統 1 的電路方塊（circuit block）示意圖。認證系統 1 包含服務裝置 10 及使用者

裝置 11。服務裝置 10 包含電子紙 100、處理器 101 及非揮發性儲存（non-volatile storage）裝置 102。依照設計需求，在一些實施例中，服務裝置 10 可以包括嵌入式設備，而電子紙 100 被配置在嵌入式設備。所述嵌入式設備包括路由器（router）、無線接入點（Wireless access point）設備與伺服器其中至少一者。

【0011】 非揮發性儲存裝置 102 可以儲存應用程式以及（或是）資料。依照設計需求，非揮發性儲存裝置 102 可包含任何類型的儲存裝置，例如固定式儲存裝置或可移動式儲存裝置。舉例來說，在一些實施例中，非揮發性儲存裝置 102 可包含唯讀記憶體（read-only memory，ROM）、快閃記憶體（FLASH memory）、硬碟（hard disk drive，HDD）、固態硬碟（solid state drive，SSD）或其他儲存裝置，或上述儲存裝置的組合。

【0012】 處理器 101 耦接於電子紙 100 及非揮發性儲存裝置 102。處理器 101 可以存取非揮發性儲存裝置 102 中儲存的資料。處理器 101 可以是透過硬體描述語言（Hardware Description Language, HDL）或是其他設計方式來實現的硬體電路。依照設計需求，處理器 101 可以包含現場可程式邏輯門陣列（Field Programmable Gate Array，FPGA）、複雜可程式邏輯裝置（Complex Programmable Logic Device，CPLD）或是特殊應用積體電路（Application-specific Integrated Circuit，ASIC）。

【0013】 處理器 101 還可以控制電子紙 100，以將認證資訊顯示於電子紙 100 上。電子紙 100 被配置在服務裝置 10 上。電子紙 100

具有低功率消耗的特性。在斷電後，電子紙 100 可以長時間持續顯示所述認證資訊以及（或是）其他資訊或圖形。電子紙 100 的實施細節可以依照設計需求來決定。舉例來說，在一些實施例中，電子紙 100 可以包括電泳顯示器（electrophoretic display，EPD）、膽固醇液晶顯示器（cholesteric liquid crystal display， ChLCD）或是其他顯示器。電子紙 100 可依據不同設計需求而包含單一個顯示器或多個顯示器。

【0014】 依照應用需求，使用者裝置 11 可以包含移動台、高級移動台（Advanced Mobile Station，AMS）、伺服器、客戶端設備、桌上型電腦、筆記型電腦、網路型電腦、工作站、個人數位助理（personal digital assistant，PDA）、個人電腦（personal computer，PC）、平板電腦、掃描儀、電話裝置、呼叫器、照相機、電視、掌上型遊戲機等。使用者裝置 11 可經由非電性通道 12 而從電子紙 100 取得認證資訊。

【0015】 舉例來說，在一些實施例中，所述「從電子紙 100 取得認證資訊」包括：由使用者裝置 11 提供使用者介面，其中在使用者視覺地從電子紙 100 閱讀所述認證資訊後，使用者可以將所述認證資訊輸入至使用者裝置 11 的使用者介面。在另一些實施例中，所述「從電子紙 100 取得認證資訊」包括：由電子紙 100 顯示所述認證資訊；由使用者裝置 11 拍攝被顯示在電子紙 100 上的認證資訊；以及由使用者裝置 11 辨識所述認證資訊（例如進行影像辨識或是光學字元辨識）。在又一些實施例中，所述「從電子紙 100

取得認證資訊」包括：由電子紙 100 顯示載有認證資訊的條碼（例如二維條碼）；由使用者裝置 11 拍攝被顯示在電子紙 100 上的條碼；以及由使用者裝置 11 從所述條碼獲得所述認證資訊。

【0016】 使用者裝置 11 可以使用被顯示在電子紙 100 上的認證資訊，而透過電性通道 13（例如網際網路）進行使用者裝置 11 與服務裝置 10 之間的認證操作。依照應用需求，在一些實施例中，所述認證操作包括「系統登入操作」、「密鑰認證操作」與「建立通訊連接操作」其中至少一者。舉例來說，在一實施例中，使用者裝置 11 可以在成功完成所述認證操作後取得服務裝置 10 的系統服務。或者，使用者裝置 11 可透過服務裝置 10 的認證，進而建立與其他裝置的服務。換言之，認證系統 1 中的使用者裝置 11 可透過認證方法與服務裝置 10 進行認證，進而取得服務裝置 10（例如為路由器、無線接入點設備與/或伺服器）的服務。

【0017】 服務裝置 10 可不須透過電性通道 13（例如網際網路）來提供認證資訊至使用者裝置 11。使用者裝置 11 可經由非電性通道 12 而從電子紙 100 取得認證資訊。非法裝置無法監聽非電性通道 12，亦無法從監聽非電性通道 12 擷取認證資訊。因此，可避免服務裝置 10 所提供的認證資訊被截取，進而有效改善認證系統 1 的資訊安全。

【0018】 圖 2 為本發明實施例一認證方法的流程示意圖。圖 2 所繪示的認證方法包含步驟 S20～S22，且可由圖 1 所繪示的認證系統 1 所執行。請參考圖 1 與圖 2，在步驟 S20 中，服務裝置 10 的

處理器 101 會將認證資訊顯示於配置在服務裝置 10 的電子紙 100 上。顯示於電子紙 100 上的認證資訊可為各種適合的資料形式。舉例來說，在一些實施例中，認證資訊可包含使用者帳號（用戶名稱）、密碼以及（或是）其他資訊。所述認證資訊可以透過文字、圖形或其他適合的方式顯示於電子紙 100 上。當認證資訊以文字顯示時，認證資訊可為未加密（或加密）的文字，以記載（或攜帶）認證資訊的內容。當認證資訊以圖形顯示時，依照設計需求，所述圖形可以包括一維條碼、二維條碼、特殊編碼形式的圖形以及（或是）其他圖形。本發明並不限制電子紙 100 上顯示的認證資訊形式。

【0019】 在步驟 S21 中，使用者裝置 11 可從電子紙 100 上獲取認證資訊。使用者裝置 11 可透過適合的方式來獲得顯示在電子紙 100 上的認證資訊。舉例而言，在認證資訊包含文字資訊的情況下，在使用者視覺地從電子紙 100 閱讀認證資訊後，使用者可以將認證資訊輸入至使用者裝置 11 所提供的使用者介面，使得使用者裝置 11 可以取得顯示在電子紙 100 上的認證資訊。在另一些實施例中，在認證資訊包含文字資訊、圖形資訊或兩者的組合的情況下，使用者裝置 11 可拍攝被顯示在電子紙 100 上的認證資訊，然後使用者裝置 11 對拍攝結果（相片）進行辨識以獲取認證資訊。在又一些實施例中，步驟 S21 包括：由電子紙 100 顯示載有認證資訊的條碼（例如二維條碼）；由使用者裝置 11 拍攝被顯示在電子紙 100 上的條碼；以及由使用者裝置 11 從所述條碼獲得所述認證資

訊。

【0020】 在步驟 S22 中，使用者裝置 11 可以使用被顯示在電子紙 100 上的認證資訊，進行使用者裝置 11 與服務裝置 10 之間的認證操作。使用者裝置 11 依據所述認證資訊可與服務裝置 10 進行兩者之間的認證操作。舉例而言，使用者裝置 11 與服務裝置 10 兩者之間所進行的認證操作可包含「系統登入操作」、「密鑰認證操作」與「建立通訊連接操作」中的至少一者。

【0021】 在一實施例中，圖 2 所繪示的認證方法可應用於「系統登入操作」。亦即，使用者裝置 11 可以使用用戶名稱與密碼登入服務裝置 10，以設定/控制服務裝置 10。在步驟 S20 中，服務裝置 10 的處理器 101 會將用戶名稱與密碼（認證資訊）顯示於電子紙 100 上。在步驟 S21 中，使用者裝置 11 可透過適合的方式從電子紙 100 上獲取用戶名稱與密碼（認證資訊）。在步驟 S22 中，藉由使用被顯示在電子紙 100 上的用戶名稱與密碼（認證資訊），使用者裝置 11 可以登入服務裝置 10，以設定/控制服務裝置 10。

【0022】 在另一實施例中，服務裝置 10 可以包括無線接入點（Wireless access point）設備。服務裝置 10 可以提供服務集識別碼（Service Set ID，SSID）以及密碼給使用者裝置 11，以便於使用者裝置 11 連接至服務裝置 10 所提供的無線網路（建立通訊連接操作）。在步驟 S20 中，服務裝置 10 的處理器 101 會將服務集識別碼（SSID）以及密碼（認證資訊）顯示於電子紙 100 上。在步驟 S21 中，使用者裝置 11 可透過適合的方式從服務裝置 10 的

電子紙 100 上取得 SSID 以及密碼（認證資訊）。在步驟 S22 中，藉由使用被顯示在電子紙 100 上的 SSID 與密碼（認證資訊），使用者裝置 11 可連接至服務裝置 10 所提供的無線網路，進而取得網路服務（建立通訊連接操作）。

【0023】 在再一實施例中，圖 2 所繪示的認證方法可應用於網路喚醒（Wake on Lan，WOL）的認證操作。舉例來說，服務裝置 10 可包含連接至電性通道 13（例如網際網路）的網路附加儲存（Network Attached Storage，NAS）裝置。在服務裝置 10 進入休眠狀態之前，服務裝置 10 可將認證資訊顯示於配置在服務裝置 10 的電子紙 100 上（步驟 S20）。所述認證資訊可包含（例如但不限於）服務裝置 10 的 MAC 地址、IP 地址、魔法封包（MAGICPACKET）以及（或是）其他適合用來喚醒服務裝置 10 的內容。在步驟 S21 中，使用者裝置 11 可透過適合的方式從服務裝置 10 的電子紙 100 上取得用來喚醒服務裝置 10 的認證資訊。在步驟 S22 中，藉由使用被顯示在電子紙 100 上的認證資訊，使用者裝置 11 可以經由電性通道 13（例如網際網路）進行使用者裝置 11 與服務裝置 10 之間的認證操作，以喚醒服務裝置 10。

【0024】 在又一實施例中，圖 2 所繪示的認證方法可應用在空間定位的認證操作。詳細而言，在本實施例中，服務裝置 10 可為伺服器裝置，而服務裝置 10 具有設置在空間中的電子紙 100。在步驟 S20 中，服務裝置 10 可將包含有地圖、路標或位置資訊的單一個或多個認證資訊顯示在電子紙 100 上。在步驟 S21 中，使用者

裝置 11 可透過適合的方式從電子紙 100 上獲取所述認證資訊。在步驟 S22 中，使用者裝置 11 可依據需求選擇認證資訊。藉由使用被顯示在電子紙 100 上的所述認證資訊，使用者裝置 11 可以向服務裝置 10 進行認證操作，以得到相對應的位置資訊。詳細而言，電子紙 100 顯示的室內地圖可具有（例如但不限於）地標圖示、圖形代碼或文字資訊，分別對應於室內的不同地點。因此，在步驟 S22 中，使用者裝置 11 可依據電子紙 100 上顯示的位置資訊進行查詢，進而取得使用者裝置 11 所在位置的相關資訊。

【0025】 圖 3 為本發明另一實施例的一認證方法的流程示意圖。圖 3 所繪示的認證方法包含步驟 S30～S34。請參考圖 1 與圖 3，在步驟 S30 中，服務裝置 10 的處理器 101 可產生密碼，並將包含所述密碼的認證資訊顯示於被配置在服務裝置 10 的電子紙 100 上，以在不變更原帳號（原用戶名稱）的情況下進行變更密碼的認證操作。或者，在另一實施例中，服務裝置 10 的處理器 101 可在步驟 S30 中產生新帳號（新用戶名稱）及新密碼以取代原帳號及原密碼，並將包含新帳號及新密碼的認證資訊顯示於被配置在服務裝置 10 的電子紙 100 上。基於設計需求以及（或是）應用需求，在一些應用情境中，處理器 101 可以只刪除原密碼而保留原帳號。在另一些應用情境中，處理器 101 可以刪除原帳號和原密碼都刪除。舉例來說，假設系統只有一個帳號，而且是超級用戶（擁有管理權限的帳號），那麼處理器 101 就不必修改原帳號，只要修改密碼即可。在一些實施例中，系統可以存在多個帳號，或者系統

允許修改超級用戶的名稱，那麼處理器 101 在步驟 S30 中可以創建新帳號並且刪除原帳號，或者修改超級用戶的名稱。

【0026】 步驟 S30 的「產生密碼」的方式可以依照設計需求來制定。舉例而言，服務裝置 10 的處理器 101 可以是以偽隨機（Pseudo-Random）或其他適合的方式產生新密碼。新密碼（認證資訊）可以透過文字、圖形或其他適合的方式顯示於電子紙 100。在另一實施例中，服務裝置 10 的處理器 101 還可以在步驟 S30 中產生新帳號(認證資訊)。步驟 S30 產生新帳號的方式可以參照「產生密碼」的相關說明來類推，故不再贅述。圖 3 所示步驟 S30 可以參照圖 2 所示步驟 S20 的相關說明而將認證資訊顯示於電子紙 100，故不再贅述。

【0027】 在步驟 S31 中，服務裝置 10 的處理器 101 會將密碼（明文）進行加密而產生經加密密碼，並將經加密密碼儲存在非揮發性儲存裝置 102 中。舉例而言，處理器 101 可使用單向加密演算法或是其他適合的加密演算法來對步驟 S30 所產生的密碼(明文）進行加密而產生經加密密碼。如此一來，即使服務裝置 10 被非法裝置入侵而造成經加密密碼外洩，非法裝置亦無法獲知密碼（明文）。在一實施例中，為了加強認證系統 1 的安全性，當處理器 101 將所述經加密密碼顯示於電子紙 100 後，處理器 101 可清除暫存器（未繪示於圖 1 中）的暫存資料，以完全清除服務裝置 10 中所儲存的未經加密密碼。

【0028】 在步驟 S32 中，使用者裝置 11 可從電子紙 100 獲得認證

資訊（包括帳號（用戶名稱）與/或密碼（明文））。圖 3 所示步驟 S32 可以參照圖 2 所示步驟 S21 的相關說明，故不再贅述。接著，在步驟 S33 中，使用者裝置 11 可經由電性通道 13(例如網際網路）傳送帳號（用戶名稱）與密碼給服務裝置 10，以便登入服務裝置 10。圖 3 所示步驟 S33 與 S34 可以參照圖 2 所示步驟 S22 的相關說明。

【0029】 在步驟 S34 中，服務裝置 10 的處理器 101 可針對使用者裝置 11 所傳送的密碼進行加密，來進行認證。詳細而言，服務裝置 10 可將使用者裝置 11 所傳送的密碼以相同於步驟 S31 中的加密方式（加密演算法）進行加密，而產生經加密資料。服務裝置 10 在步驟 S34 中可以檢查所述經加密資料。服務裝置 10 可以判斷所述經加密資料（使用者裝置 11 所傳送的密碼經加密後的結果）與所述經加密密碼（非揮發性儲存裝置 102 中所儲存的經加密密碼）是否一致。當所述經加密資料與被保存在非揮發性儲存裝置 102 的所述經加密密碼一致時，則處理器 101 可以判斷「登入成功」。反之，當所述經加密資料與被保存在非揮發性儲存裝置 102 中的所述經加密密碼不一致時，則處理器 101 判斷「登入失敗」。

【0030】 簡言之，圖 3 所繪示的認證方法可避免在服務裝置 10 中儲存未經加密的密碼。另外，顯示於電子紙 100 上的認證資訊亦無法被服務裝置 10 進行讀取，故即使服務裝置 10 遭到入侵也可以保障使用者密碼不會外洩，進而有效改善認證系統 1 的資訊安全。

【0031】 圖 4 為本發明另一實施例一認證方法的流程示意圖。認證系統 1 可透過圖 4 所繪示的認證方法檢查認證資訊中的密碼是否有定期更新，以加強認證系統 1 的資訊安全。圖 4 所繪示的認證方法包含步驟 S40～S42。圖 4 中的步驟 S40～S41 相似於圖 3 中的步驟 S30～S31，故相關內容請參考圖 3 所示步驟 S30～S31 的相關說明，於此不另贅述。

【0032】 請參考圖 1 與圖 4，在步驟 S42 中，服務裝置 10 的處理器 101 可檢查關於密碼的先前修改時間。詳細而言，處理器 101 還可於每次產生新密碼的時候記錄時間，並將所述時間儲存於非揮發性儲存裝置 102 中作為「先前修改時間」。因此，處理器 101 可比較目前時間與先前修改時間（前次服務裝置 10 產生新密碼的時間）以獲得兩者的間隔時間長度。處理器 101 還可以判斷所述先前修改時間至目前時間的時間長度是否大於門檻。所述門檻可以依照設計需求以及（或是）應用需求來設置。當所述時間長度小於或等於門檻時（步驟 S42 的判斷結果為「先前修改時間未逾時」），則可處理器 101 可以重複進行步驟 S42，以持續監控認證的密碼是否有定期更新。

【0033】 反之，當所述間隔時間長度超過（大於）所述門檻時（步驟 S42 的判斷結果為「先前修改時間逾時」），則服務裝置 10 的處理器 101 可以再一次進行步驟 S40 以更新認證的密碼。在步驟 S40 中，服務裝置 10 的處理器 101 可產生新密碼以取代原密碼，並且將新密碼顯示於被配置在服務裝置 10 的電子紙 100 上。或者，在

步驟 S40 中，服務裝置 10 的處理器 101 可產生新帳號及新密碼以取代原帳號及密碼，並將新帳號及新密碼顯示於被配置在服務裝置 10 的電子紙 100 上。如此一來，服務裝置 10 可定期更新使用者裝置 11 認證的密碼，並透過於電子紙 100 上顯示更新的認證資訊，進而有效改善認證系統 1 的資訊安全。

【0034】 另外，由於認證資訊中可包含密碼之外的資訊，因此在步驟 S40 中，服務裝置 10 的處理器 101 將新密碼顯示於配置在服務裝置 10 的電子紙 100 上時，可透過不同的方式來更新電子紙 100 上的顯示畫面。舉例而言，當電子紙 100 具有多個顯示螢幕時，服務裝置 10 可更新多個顯示螢幕中的部份或全部所顯示的認證資訊。或者，在電子紙 100 具有可局部更新的畫面的功能的情況下，服務裝置 100 亦可更新電子紙 100 上顯示密碼的特定區域，而不更新電子紙 100 的其他區域。

【0035】 圖 3 中的步驟 S32～S34 當然也可應用於圖 4 所繪示的認證方法中。詳細而言，在步驟 S41 完成之後，使用者裝置 11 可從電子紙 100 獲得認證資訊（步驟 S32），以及經由電性通道 13 傳送帳號與密碼給服務裝置 10 以便登入服務裝置 10（步驟 S33）。服務裝置 10 的處理器 101 可以加密使用者裝置 11 所傳送來的密碼而產生經加密資料，並檢查所述經加密資料與非揮發性儲存裝置 102 中所儲存的經加密密碼是否一致（步驟 S34）。

【0036】 圖 5 為本發明另一實施例一認證方法的流程示意圖。圖 5 包含步驟 S50～S55。整體而言，圖 5 所繪示的認證方法可透過服

務裝置 10 於電子紙 100 上顯示認證資訊，讓使用者裝置 11 可檢查服務裝置 10 是否為合法裝置。圖 5 所示實施例將使用非對稱加密演算法來進行認證操作。

【0037】 請參考圖 1 與圖 5，在步驟 S50 中，使用者裝置 11 可向服務裝置 10 的處理器 101 請求建立通訊連接，並提供識別資訊至服務裝置 10。依照設計需求，在一些實施例中，使用者裝置 11 所提供的識別資訊可以是與使用者裝置 11 相關的識別資訊。舉例而言，與使用者裝置 11 相關的所述識別資訊可包含（例如但不限制於）使用者裝置 11 的型號、用戶身分模組（Subscriber Identity Module，SIM）卡資料、網路位址、使用者裝置 11 發出請求的時間戳、使用者裝置 11 的定位位置、或者是其他關於使用者裝置 11 端的資訊。在另一些實施例中，使用者裝置 11 所提供的識別資訊可以是任何資料或數值。舉例來說，使用者裝置 11 所提供的識別資訊可以包含偽隨機（Pseudo-Random）值或是其他無關於使用者裝置 11 的任何資料或數值。在將識別資訊提供給服務裝置 10 後，使用者裝置 11 依然保留這個識別資訊以便於步驟 S55 使用。

【0038】 在步驟 S51 中，服務裝置 10 的處理器 101 以服務裝置 10 的私鑰（private key）加密使用者裝置 11 所提供的識別資訊，以產生經加密資訊。詳細而言，服務裝置 10 的處理器 101 可以利用非對稱加密演算法產生互相對應的公鑰及私鑰，並以私鑰對使用者裝置 11 所提供的識別資訊進行加密。

【0039】 在步驟 S52 中，服務裝置 10 的處理器 101 可將認證資訊

顯示於電子紙 100 上。在本實施例中，顯示於電子紙 100 的認證資訊可以包含所述經加密資訊以及服務裝置 10 的公鑰。圖 5 所示步驟 S52 可以參照圖 2 所示步驟 S20 的相關說明而將認證資訊顯示於電子紙 100，故不再贅述。

【0040】 在步驟 S53 中，使用者裝置 11 可從電子紙 100 獲取認證資訊（包括所述經加密資訊以及服務裝置 10 的公鑰）。圖 5 所示步驟 S53 可以參照圖 2 所示步驟 S21 的相關說明，使得使用者裝置 11 可透過適合的方式來獲得顯示在電子紙 100 上的認證資訊，故不再贅述步驟 S53 的細節。

【0041】 在步驟 S54 中，使用者裝置 11 可以利用服務裝置 10 的公鑰解密所述經加密資訊，以產生經解密資訊。由於所述經加密資訊是服務裝置 10 以私鑰進行加密所產生的，故使用者裝置 11 使用服務裝置 10 的公鑰應可正確解密所述經加密資訊。

【0042】 在步驟 S55 中，使用者裝置 11 可以檢查所述經解密資訊。如前述關於步驟 S50 的說明，在將識別資訊提供給服務裝置 10 後，使用者裝置 11 依然保留這個識別資訊。當所述經解密資訊（所述經加密資訊的解密結果）與這個識別資訊一致時，則使用者裝置 11 可以判定為「認證成功」（亦即服務裝置 10 為合法裝置）。反之，當所述經解密資訊（所述經加密資訊的解密結果）與這個識別資訊不一致時，則使用者裝置 11 可以判定為「認證失敗」（亦即服務裝置 10 為非法裝置）。

【0043】 簡言之，在圖 5 繪示的認證方法中，使用者裝置 11 可透

過以服務裝置 10 的公鑰解密經加密使用者裝置 11 資訊來判斷公鑰是否正確（密鑰認證操作）。服務裝置 10 的電子紙 100 通過非電性通道 12 提供服務裝置 10 的公鑰及經加密資訊給使用者裝置 11。圖 5 所繪示的認證方法可以避免駭客以釣魚網站的認證介面來竊取使用者裝置 11 的資訊。此外，電子紙 100 所提供的非電性通道 12 還可以避免服務裝置 10 的公鑰在網路傳輸的過程中被竊取。因此，圖 5 所繪示的認證方法可以有效避免釣魚網站竊取資料或是認證資訊的外流，進而有效改善認證系統 1 的資訊安全。

【0044】 圖 6 為本發明另一實施例一認證方法的流程示意圖。圖 6 所繪示的認證方法包含步驟 S60～S67。整體而言，圖 6 所繪示的認證方法可透過服務裝置 10 於電子紙 100 上顯示認證資訊，讓使用者裝置 11 依據認證資訊回覆服務裝置 10。服務裝置 10 可依據使用者裝置 11 的回覆內容檢查使用者裝置 11 是否為合法裝置。圖 6 所示實施例將使用非對稱加密演算法來進行認證操作。

【0045】 請參考圖 1 與圖 6，在步驟 S60 中，使用者裝置 11 可向服務裝置 10 的處理器 101 請求建立通訊連接。響應於使用者裝置 11 的請求，在步驟 S61 中，服務裝置 10 的處理器 101 可產生識別資訊。依照設計需求，在一些實施例中，服務裝置 10 所提供的識別資訊可以是與服務裝置 10 相關的識別資訊。舉例而言，與服務裝置 10 相關的所述識別資訊可包含（例如但不限制於）服務裝置 10 的系統訊息、系統名稱、系統時間、系統的網路位址等，或者是其他關於服務裝置 10 的資訊。在另一些實施例中，服務裝置 10

所提供的識別資訊可以是任何資料或數值。舉例來說，服務裝置 10 所提供的識別資訊可以包含偽隨機（Pseudo-Random）值或是其他無關於服務裝置 10 的任何資料或數值。服務裝置 10 可以保留這個識別資訊，以便於步驟 S67 使用。

【0046】 在步驟 S62 中，服務裝置 10 的處理器 101 可將認證資訊顯示於電子紙 100 上。在本實施例中，顯示於電子紙 100 的認證資訊包含所述識別資訊以及服務裝置 10 的公鑰。圖 6 所示步驟 S62 可以參照圖 2 所示步驟 S20 的相關說明而將認證資訊顯示於電子紙 100，故不再贅述。詳細而言，服務裝置 10 的處理器 101 可以利用非對稱加密演算法產生互相對應的公鑰及私鑰，並將所述公鑰以及所述識別資訊顯示於電子紙 100 上。

【0047】 在步驟 S63 中，使用者裝置 11 可從電子紙 100 獲取認證資訊（包括所述識別資訊以及服務裝置 10 的公鑰）。圖 6 所示步驟 S63 可以參照圖 2 所示步驟 S21 的相關說明，使得使用者裝置 11 可透過適合的方式來獲得顯示在電子紙 100 上的認證資訊，故不再贅述步驟 S63 的細節。

【0048】 在步驟 S64 中，使用者裝置 11 可以使用服務裝置 10 的公鑰加密所述識別資訊，以產生經加密資訊。在步驟 S65 中，使用者裝置 11 可以通過電性通道 13（例如網際網路、區域網路以及/或是其他網路）提供經加密資訊至服務裝置 10 的處理器 101，以便進行認證。由於服務裝置 10 的公鑰是通過非電性通道 12 傳輸給使用者裝置 11，故服務裝置 10 的公鑰資訊安全無虞。使用者裝

置 11 使用服務裝置 10 的公鑰對服務裝置 10 所提供的識別資訊進行加密，可產生出駭客無法偽造的經加密資訊。

【0049】 在步驟 S66 中，服務裝置 10 的處理器 101 可以使用服務裝置 10 的私鑰解密所述經加密資訊，以產生經解密資訊。由於所述經加密資訊是使用者裝置 11 以服務裝置 10 的公鑰進行加密所產生的，故服務裝置 10 使用服務裝置 10 的私鑰應可正確解密所述經加密資訊。

【0050】 在步驟 S67 中，服務裝置 10 的處理器 101 可以檢查所述經解密資訊。如前述關於步驟 S61 的說明，服務裝置 10 保留這個識別資訊，以便於步驟 S67 使用。當所述經解密資訊（所述經加密資訊的解密結果）與這個識別資訊一致時，則處理器 101 可以判定為「認證成功」（亦即使用者裝置 11 為合法裝置）。反之，當所述經解密資訊（所述經加密資訊的解密結果）與這個識別資訊不一致時，則處理器 101 可以判定為「認證失敗」（亦即使用者裝置 11 為非法裝置）。

【0051】 簡言之，在圖 6 繪示的認證方法中，使用者裝置 11 可透過服務裝置 10 的公鑰對服務裝置 10 所提供的識別資訊進行加密，並將加密結果（經加密資訊）回傳給服務裝置 10。服務裝置 10 對經加密資訊進行解密，以判斷使用者裝置 11 是否為合法裝置。服務裝置 10 的電子紙 100 通過非電性通道 12 提供認證資訊（識別資訊與服務裝置 10 的公鑰）給使用者裝置 11。圖 6 所繪示的認證方法可有效避免駭客截取公鑰與偽造公鑰，故圖 6 所繪示的認

證方法可以有效改善認證系統 1 的資訊安全。

【0052】 圖 7 為本發明另一實施例一認證方法的流程示意圖。圖 7 所繪示的認證方法包含步驟 S70～S79。整體而言，圖 7 所繪示的認證方法可以進行使用裝置 11 以及服務裝置 10 之間的雙向認證。亦即，基於服務裝置 10 的電子紙 100 所顯示的認證資訊，使用者裝置 11 可以檢查服務裝置 10 是否為合法裝置，而服務裝置 10 亦可以檢查使用者裝置 11 是否為合法裝置。

【0053】 請參考圖 1 與圖 7，在步驟 S70 中，使用者裝置 11 可向服務裝置 10 的處理器 101 請求建立通訊連接，並提供第一識別資訊至服務裝置 10。圖 7 所示步驟 S70 可以參照圖 5 所示步驟 S50 的相關說明，而步驟 S70 所述第一識別資訊可以參照步驟 S50 所述識別資訊的相關說明，故在此不予贅述。在將第一識別資訊提供給服務裝置 10 後，使用者裝置 11 依然保留這個第一識別資訊以便於步驟 S75 使用。

【0054】 在步驟 S71 中，服務裝置 10 的處理器 101 可以使用服務裝置 10 的私鑰加密使用者裝置 11 所提供的第一識別資訊，以產生第一經加密資訊。服務裝置 10 的處理器 101 在步驟 S71 中還可以產生第二識別資訊。服務裝置 10 可以保留這個第二識別資訊，以便於步驟 S79 使用。圖 7 所示步驟 S71 可以參照圖 5 所示步驟 S51 與/或圖 6 所示步驟 S61 的相關說明，步驟 S71 所述第一識別資訊與第一經加密資訊可以參照步驟 S51 所述識別資訊與經加密資訊的相關說明，而步驟 S71 所述第二識別資訊可以參照步驟 S61

所述識別資訊的相關說明，故在此不予贅述。

【0055】 在步驟 S72 中，服務裝置 10 的處理器 101 可將認證資訊顯示於電子紙 100 上。在本實施例中，顯示於電子紙 100 的認證資訊可包含服務裝置 10 的公鑰、所述第一經加密資訊及所述第二識別資訊。圖 7 所示步驟 S72 可以參照圖 5 所示步驟 S52 與/或圖 6 所示步驟 S62 的相關說明，步驟 S72 所述第一經加密資訊可以參照步驟 S52 所述經加密資訊的相關說明，而步驟 S72 所述第二識別資訊可以參照步驟 S62 所述識別資訊的相關說明，故在此不予贅述。

【0056】 在步驟 S73 中，使用者裝置 11 可從電子紙 100 獲取認證資訊（包括所述第一經加密資訊、所述第二識別資訊以及服務裝置 10 的所述公鑰）。圖 7 所示步驟 S73 可以參照圖 2 所示步驟 S21 的相關說明，使得使用者裝置 11 可透過適合的方式來獲得顯示在電子紙 100 上的認證資訊。圖 7 所示步驟 S73 可以參照圖 5 所示步驟 S53 與/或圖 6 所示步驟 S63 的相關說明，步驟 S73 所述第一經加密資訊可以參照步驟 S53 所述經加密資訊的相關說明，而步驟 S73 所述第二識別資訊可以參照步驟 S63 所述識別資訊的相關說明，故在此不予贅述。

【0057】 在步驟 S74 中，使用者裝置 11 可以利用服務裝置 10 的公鑰解密所述第一經加密資訊，以產生第一經解密資訊。圖 7 所示步驟 S74 可以參照圖 5 所示步驟 S54 的相關說明，步驟 S74 所述第一經加密資訊與第一經解密資訊可以參照步驟 S54 所述經加

密資訊與經解密資訊的相關說明，故在此不予贅述。

【0058】 在步驟 S75 中，使用者裝置 11 可以檢查所述第一經解密資訊。在步驟 S70 將第一識別資訊提供給服務裝置 10 後，使用者裝置 11 依然保留這個第一識別資訊。當所述第一經解密資訊（所述第一經加密資訊的解密結果）與這個第一識別資訊一致時，則使用者裝置 11 可以判定為「認證成功」（亦即使用者裝置 11 判定服務裝置 10 為合法裝置）。反之，當所述第一經解密資訊（所述第一經加密資訊的解密結果）與這個第一識別資訊不一致時，則使用者裝置 11 可以判定為「認證失敗」（亦即使用者裝置 11 判定服務裝置 10 為非法裝置）。圖 7 所示步驟 S75 可以參照圖 5 所示步驟 S55 的相關說明，步驟 S75 所述第一識別資訊與第一經解密資訊可以參照步驟 S55 所述識別資訊與經解密資訊的相關說明，故在此不予贅述。

【0059】 在步驟 S76 中，使用者裝置 11 可以使用服務裝置 10 的公鑰加密所述第二識別資訊，以產生第二經加密資訊。圖 7 所示步驟 S76 可以參照圖 6 所示步驟 S64 的相關說明，步驟 S76 所述第二識別資訊與第二經加密資訊可以參照步驟 S64 所述識別資訊與經加密資訊的相關說明，故在此不予贅述。

【0060】 在步驟 S77 中，使用者裝置 11 可以通過電性通道 13（例如網際網路、區域網路以及/或是其他網路）提供所述第二經加密資訊至服務裝置 10 的處理器 101，以便進行認證。圖 7 所示步驟 S77 可以參照圖 6 所示步驟 S65 的相關說明，步驟 S77 所述第二

經加密資訊可以參照步驟 S65 所述經加密資訊的相關說明，故在此不予贅述。

【0061】 在步驟 S78 中，服務裝置 10 的處理器 101 可以使用服務裝置 10 的私鑰解密所述第二經加密資訊，以產生第二經解密資訊。圖 7 所示步驟 S78 可以參照圖 6 所示步驟 S66 的相關說明，步驟 S78 所述第二經加密資訊與第二經解密資訊可以參照步驟 S66 所述經加密資訊與經解密資訊的相關說明，故在此不予贅述。

【0062】 在步驟 S79 中，服務裝置 10 的處理器 101 可以檢查所述第二經解密資訊。如前述關於步驟 S71 的說明，服務裝置 10 保留了這個第二識別資訊，以便於步驟 S79 使用。當所述第二經解密資訊（所述第二經加密資訊的解密結果）與這個第二識別資訊一致時，則處理器 101 可以判定為「認證成功」（亦即服務裝置 10 判定使用者裝置 11 為合法裝置）。反之，當所述第二經解密資訊（所述第二經加密資訊的解密結果）與這個第二識別資訊不一致時，則處理器 101 可以判定為「認證失敗」（亦即服務裝置 10 判定使用者裝置 11 為非法裝置）。圖 7 所示步驟 S79 可以參照圖 6 所示步驟 S67 的相關說明，步驟 S79 所述第二經解密資訊與第二識別資訊可以參照步驟 S67 所述經解密資訊與識別資訊的相關說明，故在此不予贅述。

【0063】 如此一來，在服務裝置 10 及使用者裝置 11 雙端都認證成功的情況下，服務裝置 10 及使用者裝置 11 之間的通訊連接可以被成功建立。

【0064】 綜上所述，基於諸實施例所述認證方法，認證系統 1 的服務裝置 10 可以使用電子紙 100 所提供的非電性通道 12 來取代電性通道 13（例如網際網路、區域網路以及/或是其他網路），以便傳輸認證資訊。利用電子紙 100 所提供認證資訊，使用者裝置 11 可以進行認證操作。透過電子紙提供（傳輸）認證資訊可有效避免認證資訊被非法截取。故，上述諸實施例的認證方法及認證系統 1 可有效改善資訊安全。

【0065】 雖然本發明已以實施例揭露如上，然其並非用以限定本發明，任何所屬技術領域中具有通常知識者，在不脫離本發明的精神和範圍內，當可作些許的更動與潤飾，故本發明的保護範圍當視後附的申請專利範圍所界定者為準。

【符號說明】

【0066】

10：服務裝置

11：使用者裝置

12：非電性通道

13：電性通道

100：電子紙

101：處理器

102：非揮發性儲存裝置

S20～S22、S30～S34、S40～S42、S50～S55、S60～S67、S70

～S79：步驟

【發明申請專利範圍】

【請求項1】 一種認證方法，包括：

由一服務裝置的一電子紙依據一認證資訊進行顯示；

由該服務裝置於該電子紙依據該認證資訊進行顯示後，清除該服務裝置的一暫存器；

由一使用者裝置從該電子紙獲取該認證資訊；以及

由該使用者裝置使用被顯示在該電子紙上的該認證資訊，以進行該使用者裝置與該服務裝置之間的一認證操作。

【請求項2】 如請求項1所述的認證方法，其中該服務裝置包括一嵌入式設備，以及該電子紙被配置在該嵌入式設備。

【請求項3】 如請求項2所述的認證方法，其中該嵌入式設備包括一路由器、一無線接入點設備與一伺服器其中至少一者。

【請求項4】 如請求項1所述的認證方法，其中該電子紙包括一電泳顯示器。

【請求項5】 如請求項1所述的認證方法，其中該認證操作包括一系統登入操作、一密鑰認證操作與一建立通訊連接操作其中至少一者。

【請求項6】 如請求項1所述的認證方法，其中所述從該電子紙獲取該認證資訊包括：

由該使用者裝置提供一使用者介面，其中在一使用者視覺地從該電子紙閱讀該認證資訊後，該使用者將該認證資訊輸入至該使用者介面。

【請求項7】 如請求項1所述的認證方法，其中所述從該電子紙獲取該認證資訊包括：

由該電子紙顯示該認證資訊；

由該使用者裝置拍攝被顯示在該電子紙上的該認證資訊；以及

由該使用者裝置辨識該認證資訊。

【請求項8】 如請求項1所述的認證方法，其中所述從該電子紙獲取該認證資訊包括：

由該電子紙顯示載有該認證資訊的一條碼；

由該使用者裝置拍攝被顯示在該電子紙上的該條碼；以及

由該使用者裝置從該條碼獲得該認證資訊。

【請求項9】 如請求項1所述的認證方法，還包含：

由該服務裝置產生一密碼，其中該認證資訊包括該密碼；

將該密碼顯示於被配置在該服務裝置的該電子紙上；

由該服務裝置加密該密碼而產生一經加密密碼；以及

由該服務裝置將該經加密密碼保存在該服務裝置內的一非揮發性儲存裝置。

【請求項10】 如請求項9所述的認證方法，其中該服務裝置是以一偽隨機方式產生該密碼。

【請求項11】 如請求項9所述的認證方法，其中該認證操作包含：

由該使用者裝置從該電子紙獲得該密碼；

由該使用者裝置傳送該密碼給該服務裝置以便登入該服務裝置；

由該服務裝置加密該使用者裝置所傳送的該密碼而產生一經加密資料；

由該服務裝置檢查該經加密資料；以及

當該經加密資料與被保存在該非揮發性儲存裝置的該經加密密碼不一致時，由該服務裝置判定登入失敗。

【請求項12】　如請求項9所述的認證方法，還包含：

由該服務裝置產生一新帳號以取代該服務裝置的一原帳號，其中該認證資訊包括該新帳號。

【請求項13】　如請求項9所述的認證方法，還包含：

檢查關於該密碼的一先前修改時間；

當該先前修改時間至一目前時間的一時間長度超過一門檻時，由該服務裝置產生一新密碼以取代該密碼，以及將該新密碼顯示於被配置在該服務裝置的該電子紙上。

【請求項14】　如請求項1所述的認證方法，其中該認證資訊包括該服務裝置的一公鑰，而該認證方法還包含：

由該使用者裝置向該服務裝置請求建立一通訊連接，並提供一識別資訊至該服務裝置；

由該服務裝置以該服務裝置的一私鑰加密該識別資訊，以產生一經加密資訊；以及

由該服務裝置將該公鑰與該經加密資訊顯示於該電子紙上。

【請求項15】　如請求項14所述的認證方法，其中該認證操作包含：

由該使用者裝置從該電子紙獲得該公鑰與該經加密資訊；

由該使用者裝置以該公鑰解密該經加密資訊，以產生一經解密資訊；

由該使用者裝置檢查該經解密資訊；以及

當該經解密資訊與該識別資訊不一致時，由該使用者裝置判定認證失敗。

【請求項16】　如請求項1所述的認證方法，其中該認證資訊包括該服務裝置的一公鑰，而該認證方法還包含：

由該使用者裝置向該服務裝置請求建立一通訊連接；

由該服務裝置產生一識別資訊，其中該認證資訊包括該識別資訊；以及

由該服務裝置將該公鑰與該識別資訊顯示於該電子紙上。

【請求項17】　如請求項16所述的認證方法，其中該認證操作包含：

由該使用者裝置從該電子紙獲得該公鑰與該識別資訊；

由該使用者裝置以該公鑰加密該識別資訊，以產生一經加密資訊；

由該使用者裝置提供該經加密資訊至該服務裝置；

由該服務裝置以該服務裝置的一私鑰解密該經加密資訊，以產生一經解密資訊；

由該服務裝置檢查該經解密資訊；以及

當該經解密資訊與該識別資訊不一致時，由該服務裝置判定認證失敗。

【請求項18】　一種認證系統，包括；

一服務裝置，包括一電子紙、一暫存器以及一處理器，其中該處理器被配置為控制該電子紙，使該電子紙依據儲存於該暫存器中的一認證資訊進行顯示；以及

一使用者裝置，用來從該電子紙獲取該認證資訊，並且使用被顯示在該電子紙上的該認證資訊，以進行該使用者裝置與該服務裝置之間的一認證操作，

其中該處理器於該電子紙依據該認證資訊進行顯示後，清除該暫存器。

【請求項19】　如請求項18所述的認證系統，其中該服務裝置包括一嵌入式設備，以及該電子紙被配置在該嵌入式設備。

【請求項20】　如請求項19所述的認證系統，其中該嵌入式設備包括一路由器、一無線接入點設備與一伺服器其中至少一者。

【請求項21】　如請求項18所述的認證系統，其中該電子紙包括一電泳顯示器。

【請求項22】　如請求項18所述的認證系統，其中該認證操作包括一系統登入操作、一密鑰認證操作與一建立通訊連接操作其中至少一者。

【請求項23】　如請求項18所述的認證系統，其中所述從該電子紙獲取該認證資訊包括：

由該使用者裝置提供一使用者介面，其中在一使用者視覺地從該電子紙閱讀該認證資訊後，該使用者將該認證資訊輸入至該使用者介面。

【請求項24】　如請求項18所述的認證系統，其中所述從該電子紙獲取該認證資訊包括：

由該電子紙顯示該認證資訊；

由該使用者裝置拍攝被顯示在該電子紙上的該認證資訊；以及

由該使用者裝置辨識該認證資訊。

【請求項25】　如請求項18所述的認證系統，其中所述從該電子紙獲取該認證資訊包括：

由該電子紙顯示載有該認證資訊的一條碼；

由該使用者裝置拍攝被顯示在該電子紙上的該條碼；以及

由該使用者裝置從該條碼獲得該認證資訊。

【請求項26】　如請求項18所述的認證系統，其中該服務裝置還包括一非揮發性儲存裝置，該處理器產生一密碼，該認證資訊包括該密碼，該處理器將該密碼顯示於被配置在該服務裝置的該電子紙上，該處理器加密該密碼而產生一經加密密碼，以及該處理器將該經加密密碼保存在該服務裝置內的該非揮發性儲存裝置。

【請求項27】　如請求項26所述的認證系統，其中該處理器是以一偽隨機方式產生該密碼。

【請求項28】　如請求項26所述的認證系統，其中該認證操作包含：

由該使用者裝置從該電子紙獲得該密碼；

由該使用者裝置傳送該密碼給該服務裝置以便登入該服務裝置；

由該處理器加密該使用者裝置所傳送的該密碼而產生一經加密資料；

由該處理器檢查該經加密資料；以及

當該經加密資料與被保存在該非揮發性儲存裝置的該經加密密碼不一致時，由該處理器判定登入失敗。

【請求項29】　如請求項26所述的認證系統，其中該處理器產生一新帳號以取代該服務裝置的一原帳號，以及該認證資訊包括該新帳號。

【請求項30】　如請求項26所述的認證系統，其中該處理器檢查關於該密碼的一先前修改時間，當該先前修改時間至一目前時間的一時間長度超過一門檻時，該處理器產生一新密碼以取代該密碼，以及將該新密碼顯示於被配置在該服務裝置的該電子紙上。

【請求項31】　如請求項18所述的認證系統，其中該認證資訊包括該服務裝置的一公鑰，

該使用者裝置向該服務裝置請求建立一通訊連接，並提供一

識別資訊至該服務裝置，

該處理器以該服務裝置的一私鑰加密該識別資訊，以產生一經加密資訊，以及

該處理器將該公鑰與該經加密資訊顯示於該服務裝置的該電子紙上。

【請求項32】　如請求項31所述的認證系統，其中該認證操作包含：

該使用者裝置從該電子紙獲得該公鑰與該經加密資訊；

該使用者裝置以該公鑰解密該經加密資訊，以產生一經解密資訊；

該使用者裝置檢查該經解密資訊；以及

當該經解密資訊與該識別資訊不一致時，該使用者裝置判定認證失敗。

【請求項33】　如請求項18所述的認證系統，其中該認證資訊包括該服務裝置的一公鑰，

該使用者裝置向該服務裝置請求建立一通訊連接；

該處理器產生一識別資訊，其中該認證資訊包括該識別資訊，以及

該處理器將該公鑰與該識別資訊顯示於該電子紙上。

【請求項34】　如請求項33所述的認證系統，其中該認證操作包含：

該使用者裝置從該電子紙獲得該公鑰與該識別資訊；

該使用者裝置以該公鑰加密該識別資訊，以產生一經加密資訊；

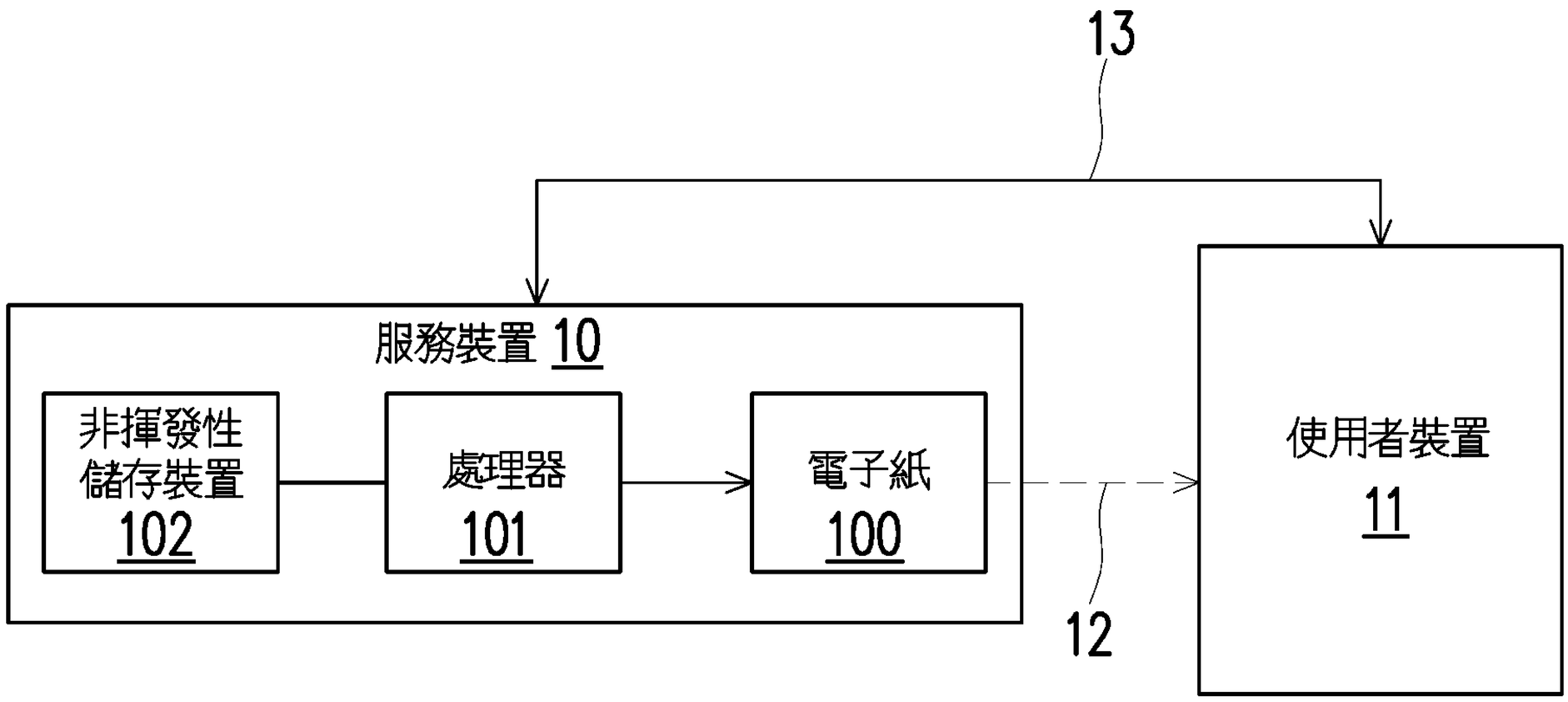
該使用者裝置提供該經加密資訊至該服務裝置進行認證；

該處理器以該服務裝置的一私鑰解密該經加密資訊，以產生一經解密資訊；

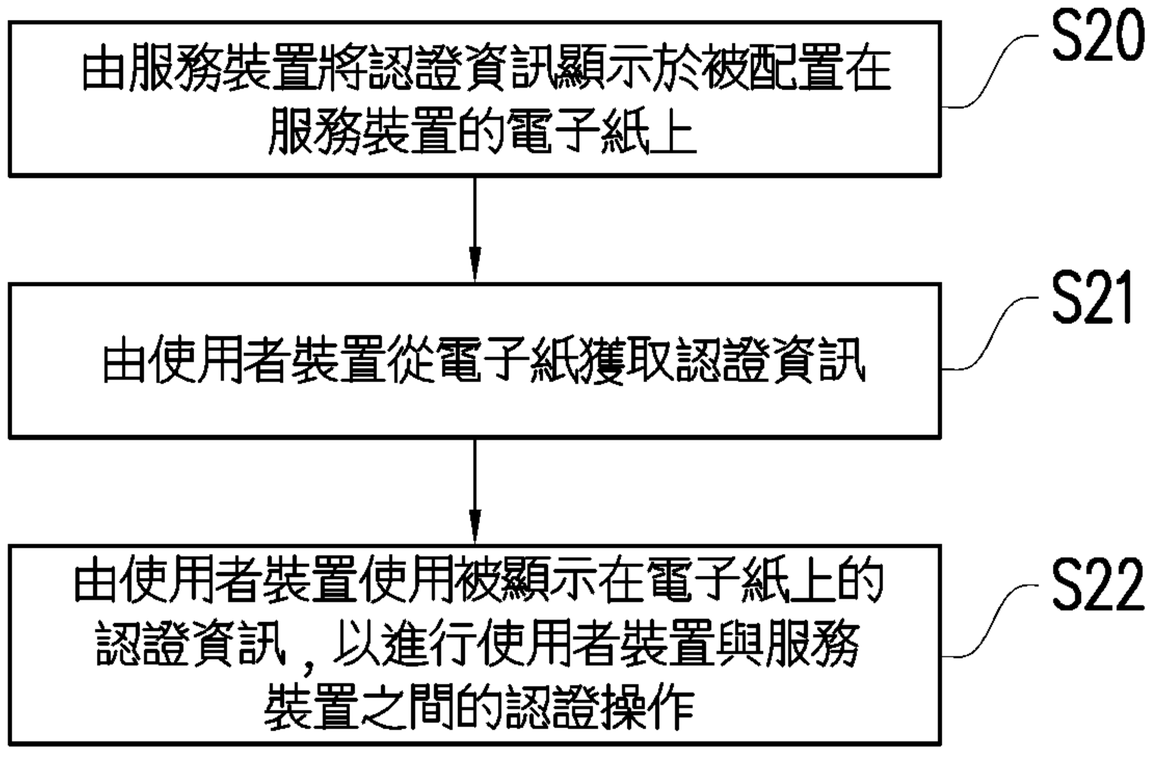
該處理器檢查該經解密資訊；以及

當該經解密資訊與該識別資訊不一致時，該處理器判定認證失敗。

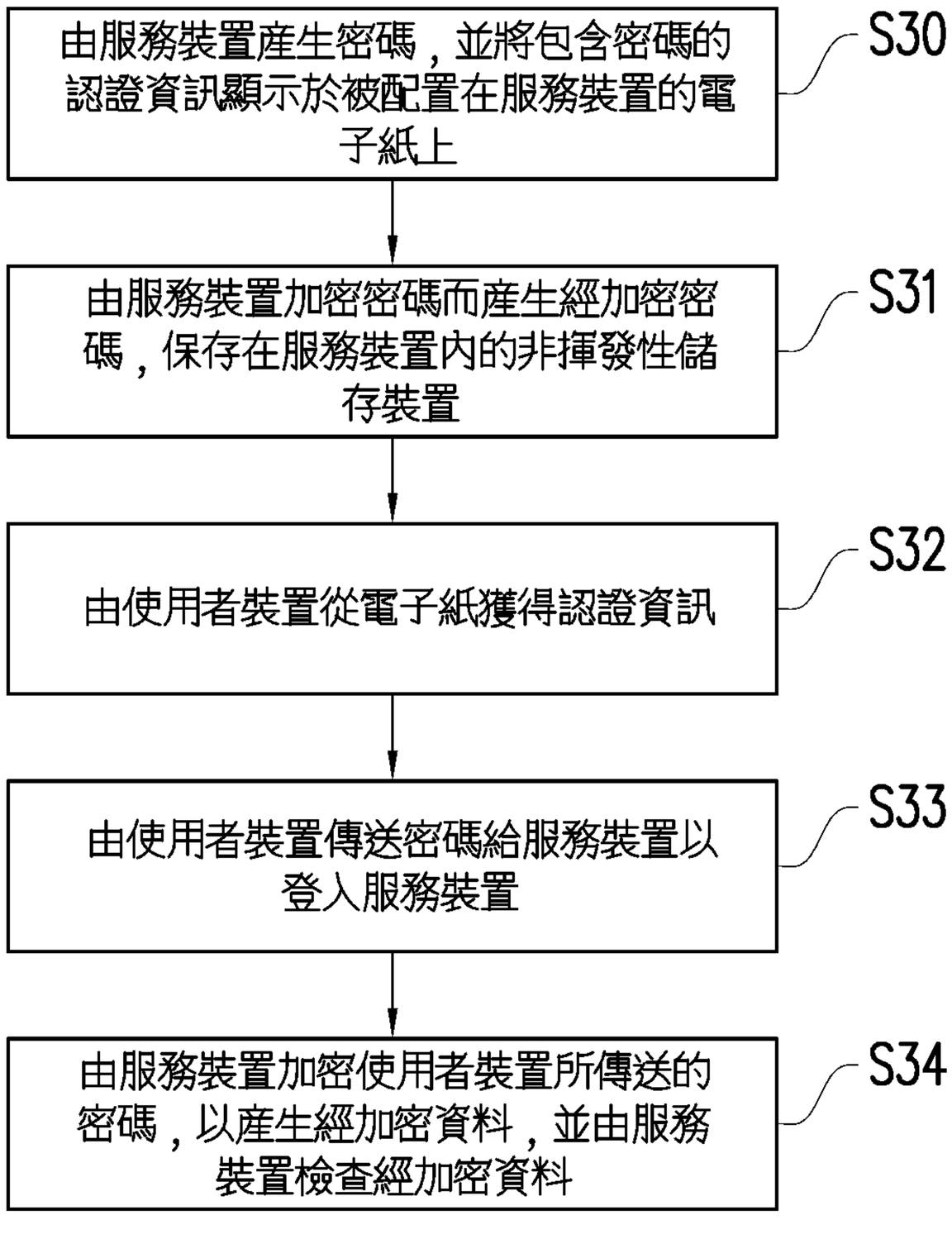
【發明圖式】


13
服務裝置 10
非揮發性
儲存裝置
102
處理器
101
電子紙
100
使用者裝置
11
12

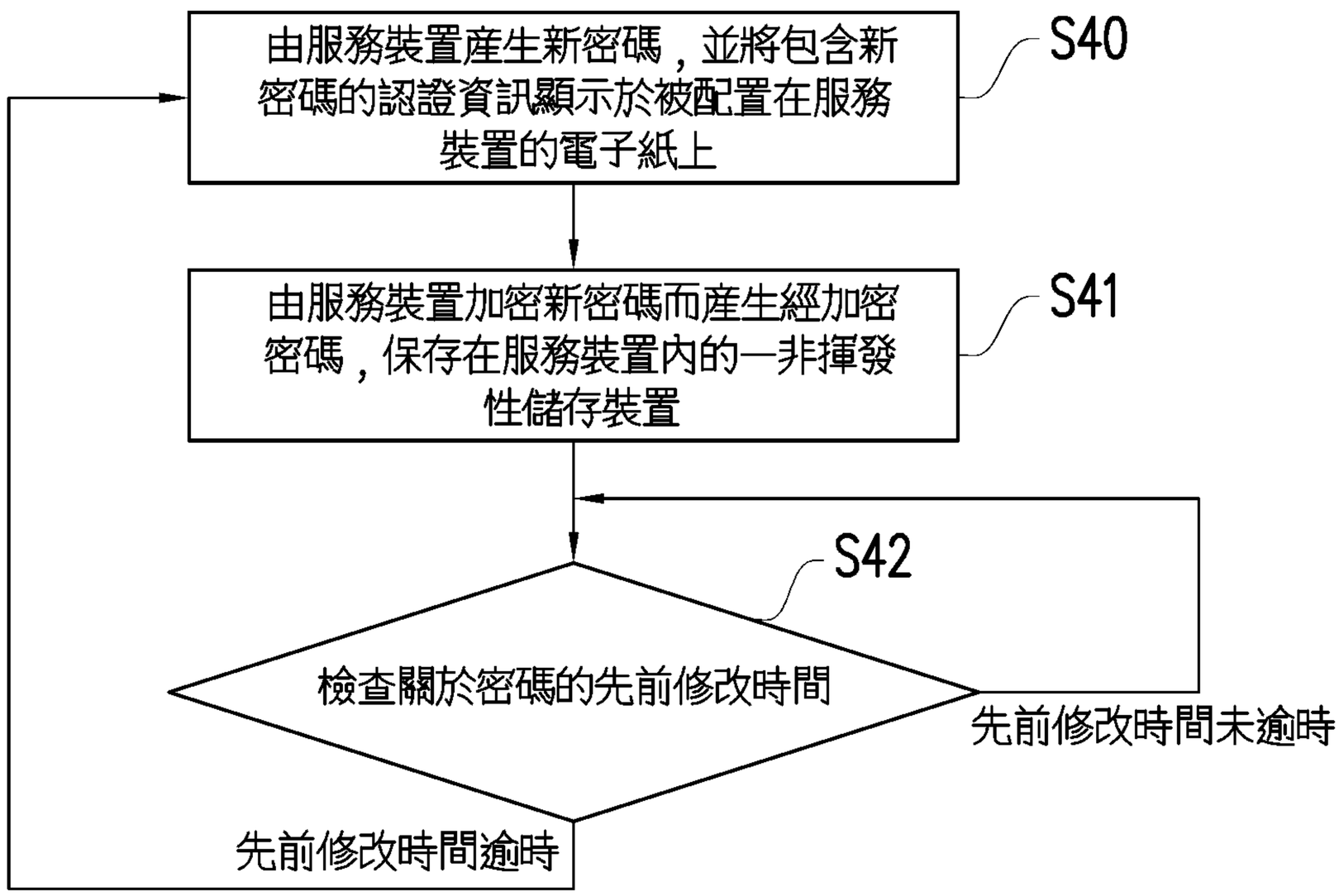
【圖1】


由服務裝置將認證資訊顯示於被配置在服務裝置的電子紙上
S20
由使用者裝置從電子紙獲取認證資訊
S21
由使用者裝置使用被顯示在電子紙上的認證資訊，以進行使用者裝置與服務裝置之間的認證操作
S22

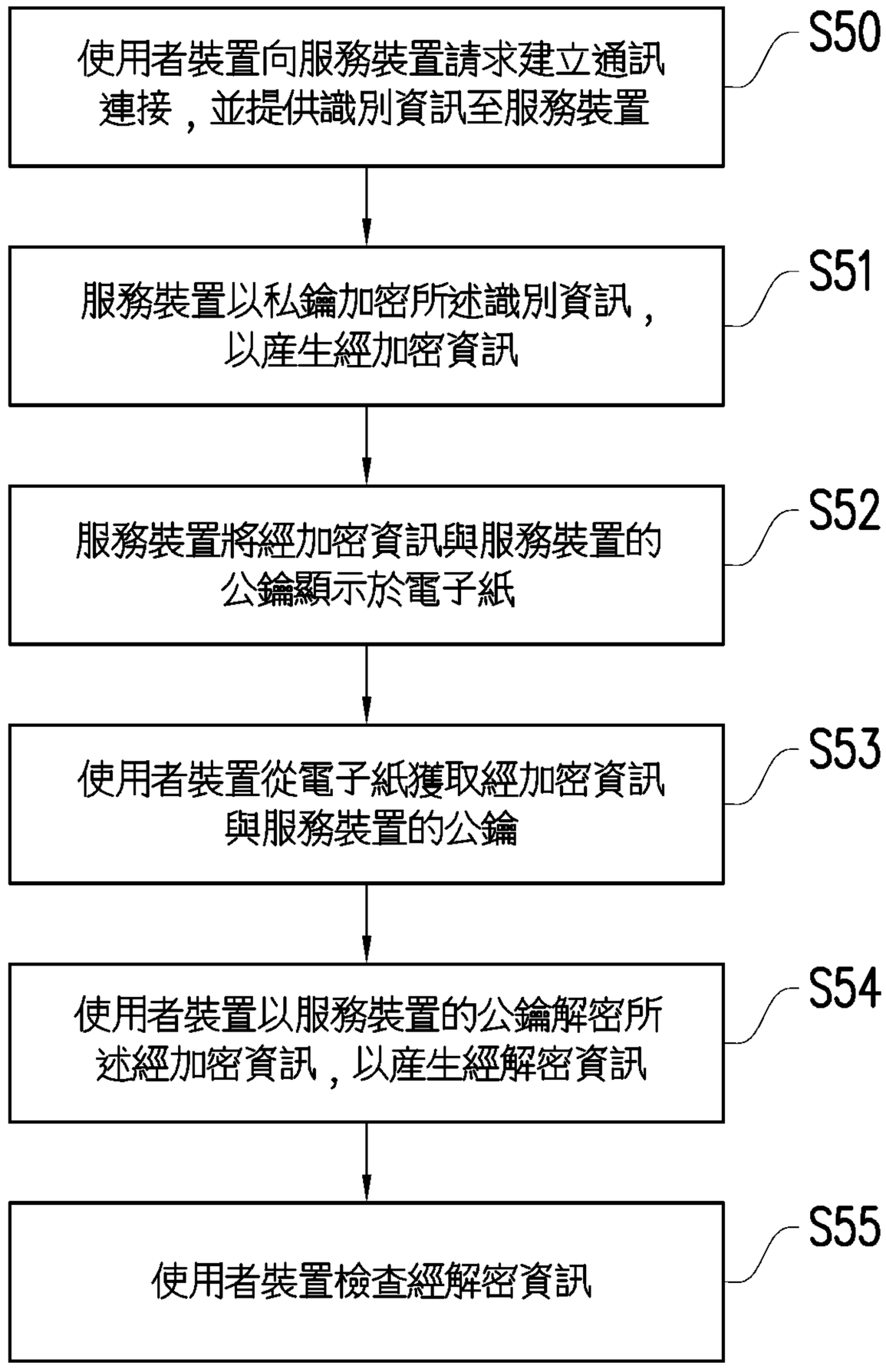
【圖2】


由服務裝置產生密碼，並將包含密碼的認證資訊顯示於被配置在服務裝置的電子紙上
S30
由服務裝置加密密碼而產生經加密密碼，保存在服務裝置內的非揮發性儲存裝置
S31
由使用者裝置從電子紙獲得認證資訊
S32
由使用者裝置傳送密碼給服務裝置以登入服務裝置
S33
由服務裝置加密使用者裝置所傳送的密碼，以產生經加密資料，並由服務裝置檢查經加密資料
S34

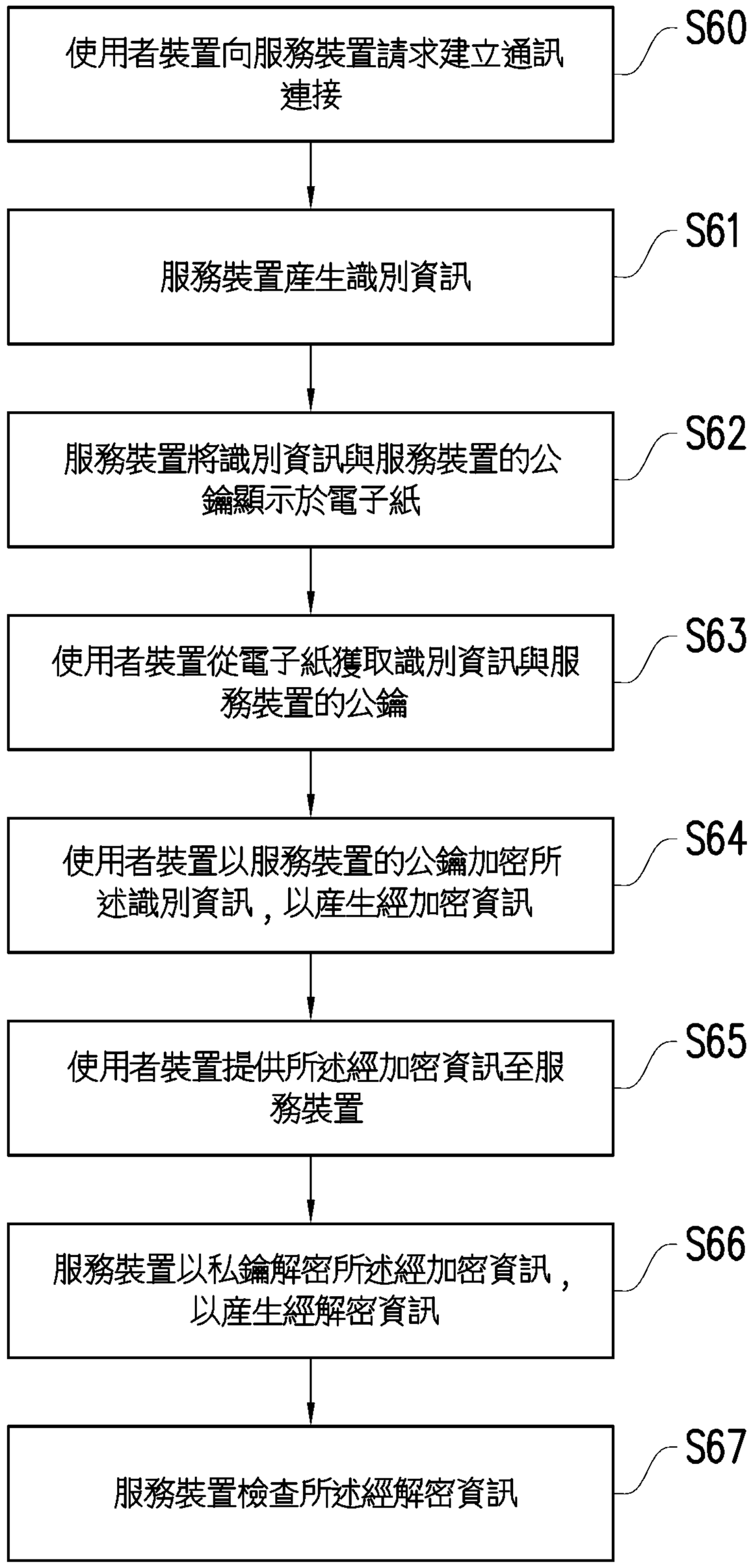
【圖3】


由服務裝置產生新密碼，並將包含新密碼的認證資訊顯示於被配置在服務裝置的電子紙上
S40
由服務裝置加密新密碼而產生經加密密碼，保存在服務裝置內的一非揮發性儲存裝置
S41
S42
檢查關於密碼的先前修改時間
先前修改時間未逾時
先前修改時間逾時

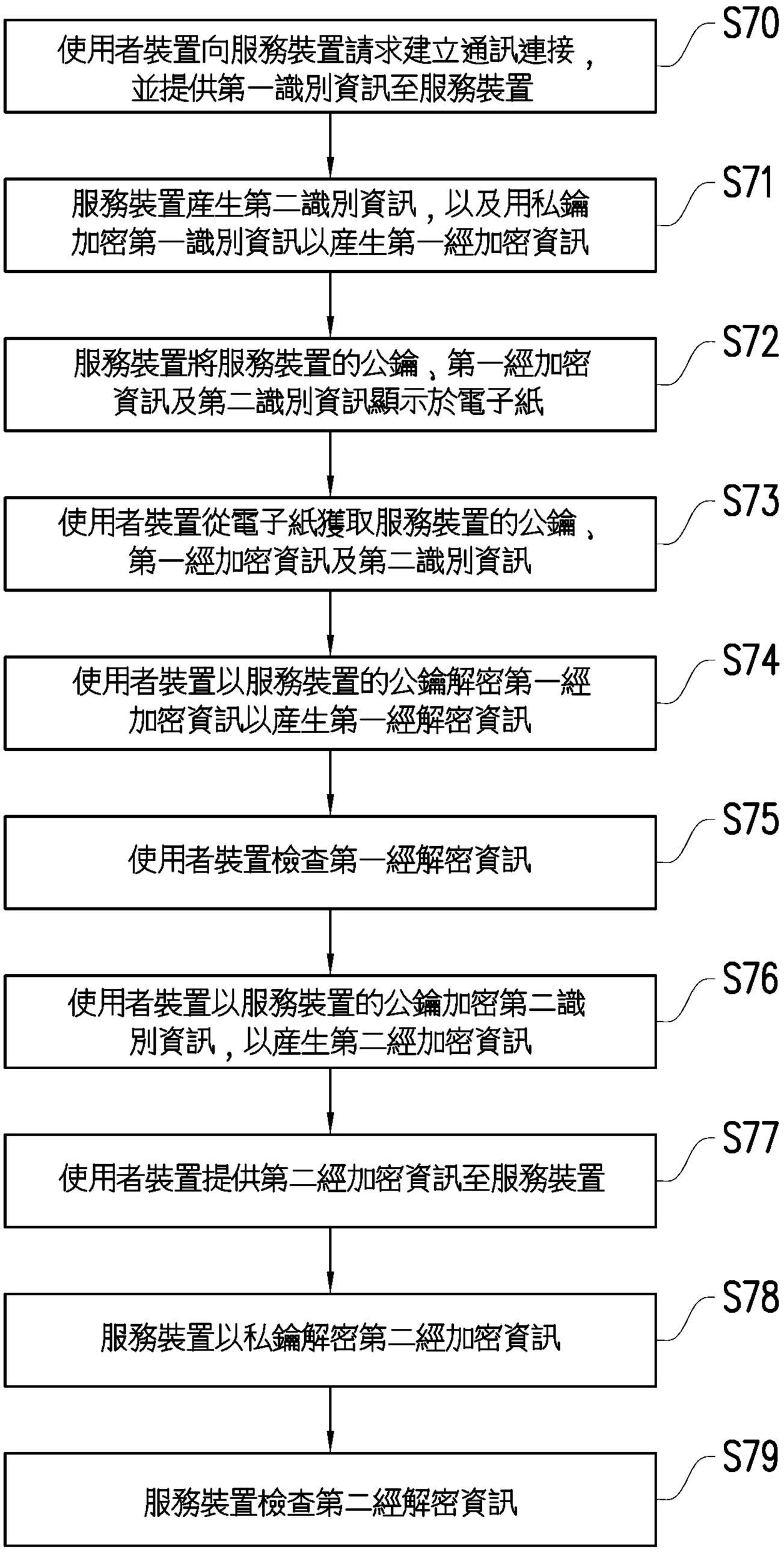
【圖4】


使用者裝置向服務裝置請求建立通訊連接，並提供識別資訊至服務裝置
S50
服務裝置以私鑰加密所述識別資訊，以產生經加密資訊
S51
服務裝置將經加密資訊與服務裝置的公鑰顯示於電子紙
S52
使用者裝置從電子紙獲取經加密資訊與服務裝置的公鑰
S53
使用者裝置以服務裝置的公鑰解密所述經加密資訊，以產生經解密資訊
S54
使用者裝置檢查經解密資訊
S55

【圖5】


使用者裝置向服務裝置請求建立通訊連接
S60
服務裝置產生識別資訊
S61
服務裝置將識別資訊與服務裝置的公鑰顯示於電子紙
S62
使用者裝置從電子紙獲取識別資訊與服務裝置的公鑰
S63
使用者裝置以服務裝置的公鑰加密所述識別資訊，以產生經加密資訊
S64
使用者裝置提供所述經加密資訊至服務裝置
S65
服務裝置以私鑰解密所述經加密資訊，以產生經解密資訊
S66
服務裝置檢查所述經解密資訊
S67

【圖6】


使用者裝置向服務裝置請求建立通訊連接，並提供第一識別資訊至服務裝置
S70
服務裝置產生第二識別資訊，以及用私鑰加密第一識別資訊以產生第一經加密資訊
S71
服務裝置將服務裝置的公鑰、第一經加密資訊及第二識別資訊顯示於電子紙
S72
使用者裝置從電子紙獲取服務裝置的公鑰，第一經加密資訊及第二識別資訊
S73
使用者裝置以服務裝置的公鑰解密第一經加密資訊以產生第一經解密資訊
S74
使用者裝置檢查第一經解密資訊
S75
使用者裝置以服務裝置的公鑰加密第二識別資訊，以產生第二經加密資訊
S76
使用者裝置提供第二經加密資訊至服務裝置
S77
服務裝置以私鑰解密第二經加密資訊
S78
服務裝置檢查第二經解密資訊
S79

【圖7】