(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 111488570 B
(45)授权公告日 2023.10.31

(21)申请号 202010291921.3

(22)申请日 2020.04.14

(65)同一申请的已公布的文献号
申请公布号 CN 111488570 A

(43)申请公布日 2020.08.04

(73)专利权人 威盛电子股份有限公司
地址 中国台湾新北市新店区中正路535号8楼

(72)发明人 徐耀忠

(74)专利代理机构 北京林达刘知识产权代理事务所(普通合伙) 11277
专利代理师 刘新宇

(51)Int.Cl.
*G06F 21/45*(2013.01)
*G06F 21/44*(2013.01)

(56)对比文件
JP 2006017906 A,2006.01.19
JP 2007264127 A,2007.10.11
JP 2009152774 A,2009.07.09
JP 2009205250 A,2009.09.10
JP 5733770 B1,2015.06.10
WO 2019087812 A1,2019.05.09
CN 101763677 A,2010.06.30
CN 101763678 A,2010.06.30
CN 101763676 A,2010.06.30

审查员 江梓琴

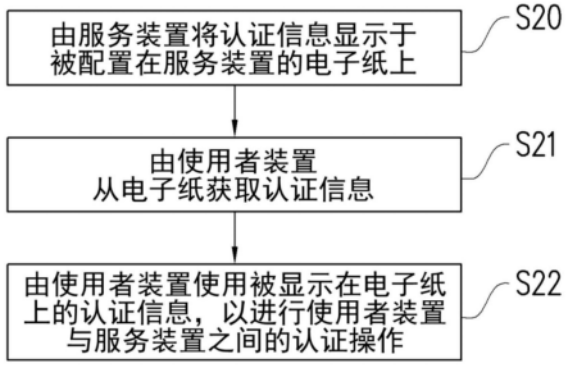
权利要求书4页 说明书10页 附图5页

(54)发明名称

# 认证方法及认证系统

(57)摘要

本发明提供一种认证方法及认证系统。认证方法包括由服务装置将认证信息显示于被配置在服务装置的电子纸上;由使用者装置从电子纸获取认证信息;以及由使用者装置使用被显示在电子纸上的认证信息,以进行使用者装置与服务装置之间的认证操作。由此,可有效改善信息安全。




CN 111488570 B

1.一种认证方法,其特征在于,包括:

由服务装置将认证信息显示于被配置在该服务装置的电子纸上;

由该服务装置在将该认证信息显示于该电子纸上之后清除该服务装置的暂存器的暂存数据;

由使用者装置经由非电性通道从该电子纸获取该认证信息;以及

由该使用者装置使用被显示在该电子纸上的该认证信息,以进行该使用者装置与该服务装置之间的认证操作,

其中,被显示在该电子纸上的该认证信息无法被该服务装置读取,该认证信息包括该服务装置的公钥,

该认证方法还包括:

由该使用者装置向该服务装置请求建立通讯连接,并提供识别信息至该服务装置;

由该服务装置以该服务装置的私钥加密该识别信息,以产生经加密信息;以及

由该服务装置将该公钥与该经加密信息显示于该电子纸上。

2.根据权利要求1所述的认证方法,其中该服务装置包括嵌入式设备,以及该电子纸被配置在该嵌入式设备。

3.根据权利要求2所述的认证方法,其中该嵌入式设备包括路由器、无线接入点设备与服务器其中至少一者。

4.根据权利要求1所述的认证方法,其中该电子纸包括电泳显示器。

5.根据权利要求1所述的认证方法,其中该认证操作包括系统登入操作、密钥认证操作与建立通讯连接操作其中至少一者。

6.根据权利要求1所述的认证方法,其中所述从该电子纸获取该认证信息包括:

由该使用者装置提供使用者接口,其中在使用者视觉地从该电子纸阅读该认证信息后,该使用者将该认证信息输入至该使用者接口。

7.根据权利要求1所述的认证方法,其中所述从该电子纸获取该认证信息包括:

由该电子纸显示该认证信息;

由该使用者装置拍摄被显示在该电子纸上的该认证信息;以及

由该使用者装置辨识该认证信息。

8.根据权利要求1所述的认证方法,其中所述从该电子纸获取该认证信息包括:

由该电子纸显示载有该认证信息的条码;

由该使用者装置拍摄被显示在该电子纸上的该条码;以及

由该使用者装置从该条码获得该认证信息。

9.根据权利要求1所述的认证方法,还包括:

由该服务装置产生密码,其中该认证信息包括该密码;

将该密码显示于被配置在该服务装置的该电子纸上;

由该服务装置加密该密码而产生经加密密码;以及

由该服务装置将该经加密密码保存在该服务装置内的非挥发性储存装置。

10.根据权利要求9所述的认证方法,其中该服务装置以伪随机方式产生该密码。

11.根据权利要求9所述的认证方法,其中该认证操作包括:

由该使用者装置从该电子纸获得该密码;

由该使用者装置传送该密码给该服务装置以便登入该服务装置；

由该服务装置加密该使用者装置所传送的该密码而产生经加密数据；

由该服务装置检查该经加密数据；以及

当该经加密数据与被保存在该非挥发性储存装置的该经加密密码不一致时，由该服务装置判定登入失败。

12.根据权利要求9所述的认证方法，还包括：

由该服务装置产生新帐号以取代该服务装置的原帐号，其中该认证信息包括该新帐号。

13.根据权利要求9所述的认证方法，还包括：

检查关于该密码的先前修改时间；

当该先前修改时间至目前时间的时间长度超过门槛时，由该服务装置产生新密码以取代该密码，以及将该新密码显示于被配置在该服务装置的该电子纸上。

14.根据权利要求1所述的认证方法，其中该认证操作包括：

由该使用者装置从该电子纸获得该公钥与该经加密信息；

由该使用者装置以该公钥解密该经加密信息，以产生经解密信息；

由该使用者装置检查该经解密信息；以及

当该经解密信息与该识别信息不一致时，由该使用者装置判定认证失败。

15.根据权利要求1所述的认证方法，该认证方法还包括：

由该使用者装置向该服务装置请求建立通讯连接；

由该服务装置产生识别信息，其中该认证信息包括该识别信息；以及

由该服务装置将该公钥与该识别信息显示于该电子纸上。

16.根据权利要求15所述的认证方法，其中该认证操作包括：

由该使用者装置从该电子纸获得该公钥与该识别信息；

由该使用者装置以该公钥加密该识别信息，以产生经加密信息；

由该使用者装置提供该经加密信息至该服务装置；

由该服务装置以该服务装置的私钥解密该经加密信息，以产生经解密信息；

由该服务装置检查该经解密信息；以及

当该经解密信息与该识别信息不一致时，由该服务装置判定认证失败。

17.一种认证系统，其特征在于，包括：

服务装置，包括电子纸、暂存器以及处理器，其中该处理器被配置为控制该电子纸，以将认证信息显示于该电子纸上；以及

使用者装置，用来经由非电性通道从该电子纸获取该认证信息，并且使用被显示在该电子纸上的该认证信息，以进行该使用者装置与该服务装置之间的认证操作，

其中，该处理器还被配置为在将该认证信息显示于该电子纸上之后清除该服务装置的该暂存器的暂存数据，

其中，被显示在该电子纸上的该认证信息无法被该服务装置读取，

其中，该认证信息包括该服务装置的公钥，

该使用者装置向该服务装置请求建立通讯连接，并提供识别信息至该服务装置；

该处理器以该服务装置的私钥加密该识别信息，以产生经加密信息；以及

该处理器将该公钥与该经加密信息显示于该电子纸上。

18.根据权利要求17所述的认证系统，其中该服务装置包括嵌入式设备，以及该电子纸被配置在该嵌入式设备。

19.根据权利要求18所述的认证系统，其中该嵌入式设备包括路由器、无线接入点设备与服务器其中至少一者。

20.根据权利要求17所述的认证系统，其中该电子纸包括电泳显示器。

21.根据权利要求17所述的认证系统，其中该认证操作包括系统登入操作、密钥认证操作与建立通讯连接操作其中至少一者。

22.根据权利要求17所述的认证系统，其中所述从该电子纸获取该认证信息包括：

由该使用者装置提供使用者接口，其中在使用者视觉地从该电子纸阅读该认证信息后，该使用者将该认证信息输入至该使用者接口。

23.根据权利要求17所述的认证系统，其中所述从该电子纸获取该认证信息包括：

由该电子纸显示该认证信息；

由该使用者装置拍摄被显示在该电子纸上的该认证信息；以及

由该使用者装置辨识该认证信息。

24.根据权利要求17所述的认证系统，其中所述从该电子纸获取该认证信息包括：

由该电子纸显示载有该认证信息的条码；

由该使用者装置拍摄被显示在该电子纸上的该条码；以及

由该使用者装置从该条码获得该认证信息。

25.根据权利要求17所述的认证系统，其中该服务装置还包括非挥发性储存装置，该处理器产生密码，该认证信息包括该密码，该处理器将该密码显示于被配置在该服务装置的该电子纸上，该处理器加密该密码而产生经加密密码，以及该处理器将该经加密密码保存在该服务装置内的该非挥发性储存装置。

26.根据权利要求25所述的认证系统，其中该处理器以伪随机方式产生该密码。

27.根据权利要求25所述的认证系统，其中该认证操作包括：

由该使用者装置从该电子纸获得该密码；

由该使用者装置传送该密码给该服务装置以便登入该服务装置；

由该处理器加密该使用者装置所传送的该密码而产生经加密数据；

由该处理器检查该经加密数据；以及

当该经加密数据与被保存在该非挥发性储存装置的该经加密密码不一致时，由该处理器判定登入失败。

28.根据权利要求25所述的认证系统，其中该处理器产生新帐号以取代该服务装置的原帐号，以及该认证信息包括该新帐号。

29.根据权利要求25所述的认证系统，其中该处理器检查关于该密码的先前修改时间，当该先前修改时间至目前时间的时间长度超过门槛时，该处理器产生新密码以取代该密码，以及将该新密码显示于被配置在该服务装置的该电子纸上。

30.根据权利要求17所述的认证系统，其中该认证操作包括：

该使用者装置从该电子纸获得该公钥与该经加密信息；

该使用者装置以该公钥解密该经加密信息，以产生经解密信息；该使用者装置检查该

经解密信息;以及

当该经解密信息与该识别信息不一致时,该使用者装置判定认证失败。

31.根据权利要求17所述的认证系统,其中,

该使用者装置向该服务装置请求建立通讯连接;

该处理器产生识别信息,其中该认证信息包括该识别信息,以及该处理器将该公钥与该识别信息显示于该电子纸上。

32.根据权利要求31所述的认证系统,其中该认证操作包括:

该使用者装置从该电子纸获得该公钥与该识别信息;

该使用者装置以该公钥加密该识别信息,以产生经加密信息;

该使用者装置提供该经加密信息至该服务装置进行认证;

该处理器以该服务装置的私钥解密该经加密信息,以产生经解密信息;该处理器检查该经解密信息;以及

当该经解密信息与该识别信息不一致时,该处理器判定认证失败。

# 认证方法及认证系统

## 技术领域

[0001] 本发明有关于一种方法及系统，且特别有关于一种认证方法及认证系统。

## 背景技术

[0002] 已知无线网络设备(服务装置)的出厂设置是使用固定的初始用户名称与固定的初始密码。使用者装置可以使用初始用户名称与初始密码登入服务装置，以设定/控制服务装置。初始用户名称与初始密码被记录在某个地方，比如记录在粘贴于设备上的贴纸，以及/或是记录在设备的说明书上。大部分使用者不会修改初始用户名称与初始密码，所以黑客很容易猜测(或者获取)已知无线网络设备的初始用户名称与初始密码。即便使用者修改用户名称与密码，大部分人都选择容易记忆的用户名称与密码(甚至是多个设备使用同一个密码)，而且也不会时常更新密码。因此，已知无线网络设备的安全系数低(亦即易被入侵)。

[0003] 此外，在传统的认证系统中，使用者装置与服务装置要利用相同的通讯网络传递(或是交换)公钥(public key)以及进行认证操作。当传递(或是交换)公钥时，非法装置可能会从所述通讯网络(电性网络，例如网际网络)拦截真公钥，并以假公钥取代真公钥。因此，传统的认证系统可能会有信息安全问题。

[0004] 再举例而言，当服务装置通过网络提供包括有密码的认证信息给使用者装置时，认证信息可能会通过网络包被第三者窃取，造成密码的外泄。或者，当使用者装置欲连接至认证页面来进行认证时，可能会连接至错误的钓鱼网站，导致密码的外泄。又或者，服务装置中所储存的帐号及密码等数据，只要服务装置遭到入侵就会造成密码的外泄。因此，传统的认证方法及认证系统存在着信息安全的风险。

## 发明内容

[0005] 本发明提供一种认证方法及认证系统，其可以提升信息安全。

[0006] 本发明的认证方法包括由服务装置将认证信息显示于被配置在服务装置的电子纸上；由使用者装置从电子纸获取认证信息；以及由使用者装置使用被显示在电子纸上的认证信息，以进行使用者装置与服务装置之间的认证操作。

[0007] 本发明的认证系统包括服务装置及使用者装置。服务装置包括电子纸以及处理器，其中处理器被配置为控制电子纸，以将认证信息显示于电子纸上。使用者装置用来从电子纸获取认证信息，并且使用被显示在电子纸上的认证信息，以进行使用者装置与服务装置之间的认证操作。

[0008] 基于上述，本发明实施例所述的认证方法及认证系统可以通过服务装置上的电子纸来传递认证信息。使用者装置使用显示在电子纸的认证信息来进行使用者装置与服务装置之间的认证操作。如此一来，服务装置所提供的认证信息可以避免在通讯网络中传递(避免非法装置从通讯网络截取认证信息)，进而有效改善认证方法及认证系统的信息安全。

## 附图说明

[0009] 图1为本发明实施例一认证系统的电路方块(circuit block)示意图。

[0010] 图2为本发明实施例一认证方法的流程示意图。

[0011] 图3为本发明另一实施例的一认证方法的流程示意图。

[0012] 图4为本发明另一实施例的一认证方法的流程示意图。

[0013] 图5为本发明另一实施例的一认证方法的流程示意图。

[0014] 图6为本发明另一实施例的一认证方法的流程示意图。

[0015] 图7为本发明另一实施例的一认证方法的流程示意图。

[0016] 其中,附图中符号的简单说明如下:

[0017] 10:服务装置;11:使用者装置;12:非电性通道;13:电性通道;100:电子纸;101:处理器;102:非挥发性储存装置;S20～S22、S30～S34、S40～S42、S50～S55、S60～S67、S70～S79:步骤。

## 具体实施方式

[0018] 请参考图1,图1为本发明实施例一认证系统1的电路方块(circuit block)示意图。认证系统1包括服务装置10及使用者装置11。服务装置10包括电子纸100、处理器101及非挥发性储存(non-volatile storage)装置102。依照设计需求,在一些实施例中,服务装置10可以包括嵌入式设备,而电子纸100被配置在嵌入式设备。所述嵌入式设备包括路由器(router)、无线接入点(Wireless access point)设备与服务器其中至少一者。

[0019] 非挥发性储存装置102可以储存应用程序以及(或是)数据。依照设计需求,非挥发性储存装置102可包括任何类型的储存装置,例如固定式储存装置或可移动式储存装置。举例来说,在一些实施例中,非挥发性储存装置102可包括只读存储器(read-only memory,ROM)、快闪存储器(FLASH memory)、硬盘(hard disk drive,HDD)、固态硬盘(solid state drive,SSD)或其他储存装置,或上述储存装置的组合。

[0020] 处理器101耦接于电子纸100及非挥发性储存装置102。处理器101可以存取非挥发性储存装置102中储存的数据。处理器101可以是通过硬件描述语言(Hardware Description Language,HDL)或是其他设计方式来实现的硬件电路。依照设计需求,处理器101可以包括现场可编程逻辑门阵列(Field Programmable Gate Array,FPGA)、复杂可编程逻辑装置(Complex Programmable Logic Device,CPLD)或是专用集成电路(Application-specific Integrated Circuit,ASIC)。

[0021] 处理器101还可以控制电子纸100,以将认证信息显示于电子纸100上。电子纸100被配置在服务装置10上。电子纸100具有低功率消耗的特性。在断电后,电子纸100可以长时间持续显示所述认证信息以及(或是)其他信息或图形。电子纸100的实施细节可以依照设计需求来决定。举例来说,在一些实施例中,电子纸100可以包括电泳显示器(electrophoretic display,EPD)、胆固醇液晶显示器(cholesteric liquid crystal display,ChLCD)或是其他显示器。电子纸100可依据不同设计需求而包括单个显示器或多个显示器。

[0022] 依照应用需求,使用者装置11可以包括移动站、高级移动站(Advanced Mobile Station,AMS)、服务器、客户端设备、桌上型计算机、笔记型计算机、网络型计算机、工作站、

个人数字助理(personal digital assistant,PDA)、个人计算机(personal computer,PC)、平板计算机、扫描仪、电话装置、呼叫器、照相机、电视、掌上型游戏机等。使用者装置11可经由非电性通道12而从电子纸100取得认证信息。

[0023] 举例来说,在一些实施例中,所述“从电子纸100取得认证信息”包括:由使用者装置11提供使用者接口,其中在使用者视觉地从电子纸100阅读所述认证信息后,使用者可以将所述认证信息输入至使用者装置11的使用者接口。在另一些实施例中,所述“从电子纸100取得认证信息”包括:由电子纸100显示所述认证信息;由使用者装置11拍摄被显示在电子纸100上的认证信息;以及由使用者装置11辨识所述认证信息(例如进行影像辨识或是光学字符辨识)。在又一些实施例中,所述“从电子纸100取得认证信息”包括:由电子纸100显示载有认证信息的条码(例如二维条码);由使用者装置11拍摄被显示在电子纸100上的条码;以及由使用者装置11从所述条码获得所述认证信息。

[0024] 使用者装置11可以使用被显示在电子纸100上的认证信息,而通过电性通道13(例如网际网络)进行使用者装置11与服务装置10之间的认证操作。依照应用需求,在一些实施例中,所述认证操作包括“系统登入操作”、“密钥认证操作”与“建立通讯连接操作”其中至少一者。举例来说,在一实施例中,使用者装置11可以在成功完成所述认证操作后取得服务装置10的系统服务。或者,使用者装置11可通过服务装置10的认证,进而建立与其他装置的服务。换言之,认证系统1中的使用者装置11可通过认证方法与服务装置10进行认证,进而取得服务装置10(例如为路由器、无线接入点设备与/或服务器)的服务。

[0025] 服务装置10可无需通过电性通道13(例如网际网络)来提供认证信息至使用者装置11。使用者装置11可经由非电性通道12而从电子纸100取得认证信息。非法装置无法监听非电性通道12,亦无法从监听非电性通道12撷取认证信息。因此,可避免服务装置10所提供的认证信息被截取,进而有效改善认证系统1的信息安全。

[0026] 图2为本发明实施例一认证方法的流程示意图。图2所绘示的认证方法包括步骤S20～S22,且可由图1所绘示的认证系统1所执行。请参考图1与图2,在步骤S20中,服务装置10的处理器101会将认证信息显示于配置在服务装置10的电子纸100上。显示于电子纸100上的认证信息可为各种适合的数据形式。举例来说,在一些实施例中,认证信息可包括使用者帐号(用户名称)、密码以及(或是)其他信息。所述认证信息可以通过文字、图形或其他适合的方式显示于电子纸100上。当认证信息以文字显示时,认证信息可为未加密(或加密)的文字,以记载(或携带)认证信息的内容。当认证信息以图形显示时,依照设计需求,所述图形可以包括一维条码、二维条码、特殊编码形式的图形以及(或是)其他图形。本发明并不限制电子纸100上显示的认证信息形式。

[0027] 在步骤S21中,使用者装置11可从电子纸100上获取认证信息。使用者装置11可通过适合的方式来获得显示在电子纸100上的认证信息。举例而言,在认证信息包括文字信息的情况下,在使用者视觉地从电子纸100阅读认证信息后,使用者可以将认证信息输入至使用者装置11所提供的使用者接口,使得使用者装置11可以取得显示在电子纸100上的认证信息。在另一些实施例中,在认证信息包括文字信息、图形信息或两者的组合的情况下,使用者装置11可拍摄被显示在电子纸100上的认证信息,然后使用者装置11对拍摄结果(相片)进行辨识以获取认证信息。在又一些实施例中,步骤S21包括:由电子纸100显示载有认证信息的条码(例如二维条码);由使用者装置11拍摄被显示在电子纸100上的条码;以及由

使用者装置11从所述条码获得所述认证信息。

[0028] 在步骤S22中，使用者装置11可以使用被显示在电子纸100上的认证信息，进行使用者装置11与服务装置10之间的认证操作。使用者装置11依据所述认证信息可与服务装置10进行两者之间的认证操作。举例而言，使用者装置11与服务装置10两者之间所进行的认证操作可包括“系统登入操作”、“密钥认证操作”与“建立通讯连接操作”中的至少一者。

[0029] 在一实施例中，图2所绘示的认证方法可应用于“系统登入操作”。亦即，使用者装置11可以使用用户名称与密码登入服务装置10，以设定/控制服务装置10。在步骤S20中，服务装置10的处理器101会将用户名称与密码(认证信息)显示于电子纸100上。在步骤S21中，使用者装置11可通过适合的方式从电子纸100上获取用户名称与密码(认证信息)。在步骤S22中，通过使用被显示在电子纸100上的用户名称与密码(认证信息)，使用者装置11可以登入服务装置10，以设定/控制服务装置10。

[0030] 在另一实施例中，服务装置10可以包括无线接入点(Wireless access point)设备。服务装置10可以提供服务集标识(Service Set ID,SSID)以及密码给使用者装置11，以便于使用者装置11连接至服务装置10所提供的无线网络(建立通讯连接操作)。在步骤S20中，服务装置10的处理器101会将服务集标识(SSID)以及密码(认证信息)显示于电子纸100上。在步骤S21中，使用者装置11可通过适合的方式从服务装置10的电子纸100上取得SSID以及密码(认证信息)。在步骤S22中，通过使用被显示在电子纸100上的SSID与密码(认证信息)，使用者装置11可连接至服务装置10所提供的无线网络，进而取得网络服务(建立通讯连接操作)。

[0031] 在再一实施例中，图2所绘示的认证方法可应用于网络唤醒(Wake on Lan,WOL)的认证操作。举例来说，服务装置10可包括连接至电性通道13(例如网际网络)的网络附加储存(Network Attached Storage,NAS)装置。在服务装置10进入休眠状态之前，服务装置10可将认证信息显示于配置在服务装置10的电子纸100上(步骤S20)。所述认证信息可包括(例如但不限于)服务装置10的MAC地址、IP地址、魔法包(MAGICPACKET)以及(或是)其他适合用来唤醒服务装置10的内容。在步骤S21中，使用者装置11可通过适合的方式从服务装置10的电子纸100上取得用来唤醒服务装置10的认证信息。在步骤S22中，通过使用被显示在电子纸100上的认证信息，使用者装置11可以经由电性通道13(例如网际网络)进行使用者装置11与服务装置10之间的认证操作，以唤醒服务装置10。

[0032] 在又一实施例中，图2所绘示的认证方法可应用在空间定位的认证操作。详细而言，在本实施例中，服务装置10可为服务器装置，而服务装置10具有设置在空间中的电子纸100。在步骤S20中，服务装置10可将包括有地图、路标或位置信息的单个或多个认证信息显示在电子纸100上。在步骤S21中，使用者装置11可通过适合的方式从电子纸100上获取所述认证信息。在步骤S22中，使用者装置11可依据需求选择认证信息。通过使用被显示在电子纸100上的所述认证信息，使用者装置11可以向服务装置10进行认证操作，以得到相对应的位置信息。详细而言，电子纸100显示的室内地图可具有(例如但不限于)地标图示、图形代码或文字信息，分别对应于室内的不同地点。因此，在步骤S22中，使用者装置11可依据电子纸100上显示的位置信息进行查询，进而取得使用者装置11所在位置的相关信息。

[0033] 图3为本发明另一实施例的一认证方法的流程示意图。图3所绘示的认证方法包括步骤S30～S34。请参考图1与图3，在步骤S30中，服务装置10的处理器101可产生密码，并将

包括所述密码的认证信息显示于被配置在服务装置10的电子纸100上，以在不变更原帐号(原用户名称)的情况下进行变更密码的认证操作。或者，在另一实施例中，服务装置10的处理器101可在步骤S30中产生新帐号(新用户名称)及新密码以取代原帐号及原密码，并将包括新帐号及新密码的认证信息显示于被配置在服务装置10的电子纸100上。基于设计需求以及(或是)应用需求，在一些应用情境中，处理器101可以只删除原密码而保留原帐号。在另一些应用情境中，处理器101可以将原帐号和原密码都删除。举例来说，假设系统只有一个帐号，而且是超级用户(拥有管理权限的帐号)，那么处理器101就不必修改原帐号，只要修改密码即可。在一些实施例中，系统可以存在多个帐号，或者系统允许修改超级用户的名称，那么处理器101在步骤S30中可以创建新帐号并且删除原帐号，或者修改超级用户的名称。

[0034] 步骤S30的“产生密码”的方式可以依照设计需求来制定。举例而言，服务装置10的处理器101可以是以伪随机(Pseudo-Random)或其他适合的方式产生新密码。新密码(认证信息)可以通过文字、图形或其他适合的方式显示于电子纸100。在另一实施例中，服务装置10的处理器101还可以在步骤S30中产生新帐号(认证信息)。步骤S30产生新帐号的方式可以参照“产生密码”的相关说明来类推，故不再赘述。图3所示步骤S30可以参照图2所示步骤S20的相关说明而将认证信息显示于电子纸100，故不再赘述。

[0035] 在步骤S31中，服务装置10的处理器101会将密码(明文)进行加密而产生经加密密码，并将经加密密码储存在非挥发性储存装置102中。举例而言，处理器101可使用单向加密演算法或是其他适合的加密演算法来对步骤S30所产生的密码(明文)进行加密而产生经加密密码。如此一来，即使服务装置10被非法装置入侵而造成经加密密码外泄，非法装置亦无法获知密码(明文)。在一实施例中，为了加强认证系统1的安全性，当处理器101将所述经加密密码显示于电子纸100后，处理器101可清除暂存器(未绘示于图1中)的暂存数据，以完全清除服务装置10中所储存的未经加密密码。

[0036] 在步骤S32中，使用者装置11可从电子纸100获得认证信息(包括帐号(用户名称)与/或密码(明文))。图3所示步骤S32可以参照图2所示步骤S21的相关说明，故不再赘述。接着，在步骤S33中，使用者装置11可经由电性通道13(例如网际网络)传送帐号(用户名称)与密码给服务装置10，以便登入服务装置10。图3所示步骤S33与S34可以参照图2所示步骤S22的相关说明。

[0037] 在步骤S34中，服务装置10的处理器101可针对使用者装置11所传送的密码进行加密，来进行认证。详细而言，服务装置10可将使用者装置11所传送的密码以相同于步骤S31中的加密方式(加密演算法)进行加密，而产生经加密数据。服务装置10在步骤S34中可以检查所述经加密数据。服务装置10可以判断所述经加密数据(使用者装置11所传送的密码经加密后的结果)与所述经加密密码(非挥发性储存装置102中所储存的经加密密码)是否一致。当所述经加密数据与被保存在非挥发性储存装置102的所述经加密密码一致时，则处理器101可以判断为“登入成功”。反之，当所述经加密数据与被保存在非挥发性储存装置102中的所述经加密密码不一致时，则处理器101判断为“登入失败”。

[0038] 简言之，图3所绘示的认证方法可避免在服务装置10中储存未经加密的密码。另外，显示于电子纸100上的认证信息亦无法被服务装置10进行读取，故即使服务装置10遭到入侵也可以保障使用者密码不会外泄，进而有效改善认证系统1的信息安全。

[0039] 图4为本发明另一实施例一认证方法的流程示意图。认证系统1可通过图4所绘示的认证方法检查认证信息中的密码是否有定期更新，以加强认证系统1的信息安全。图4所绘示的认证方法包括步骤S40～S42。图4中的步骤S40～S41相似于图3中的步骤S30～S31，故相关内容请参考图3所示步骤S30～S31的相关说明，于此不另赘述。

[0040] 请参考图1与图4，在步骤S42中，服务装置10的处理器101可检查关于密码的先前修改时间。详细而言，处理器101还可于每次产生新密码的时候记录时间，并将所述时间储存于非挥发性储存装置102中作为“先前修改时间”。因此，处理器101可比较目前时间与先前修改时间(前次服务装置10产生新密码的时间)以获得两者的间隔时间长度。处理器101还可以判断所述先前修改时间至目前时间的时间长度是否大于门槛。所述门槛可以依照设计需求以及(或是)应用需求来设置。当所述时间长度小于或等于门槛时(步骤S42的判断结果为“先前修改时间未逾时”)，则可处理器101可以重复进行步骤S42，以持续监控认证的密码是否有定期更新。

[0041] 反之，当所述间隔时间长度超过(大于)所述门槛时(步骤S42的判断结果为“先前修改时间逾时”)，则服务装置10的处理器101可以再一次进行步骤S40以更新认证的密码。在步骤S40中，服务装置10的处理器101可产生新密码以取代原密码，并且将新密码显示于被配置在服务装置10的电子纸100上。或者，在步骤S40中，服务装置10的处理器101可产生新帐号及新密码以取代原帐号及密码，并将新帐号及新密码显示于被配置在服务装置10的电子纸100上。如此一来，服务装置10可定期更新使用者装置11认证的密码，并通过于电子纸100上显示更新的认证信息，进而有效改善认证系统1的信息安全。

[0042] 另外，由于认证信息中可包括密码之外的信息，因此在步骤S40中，服务装置10的处理器101将新密码显示于配置在服务装置10的电子纸100上时，可通过不同的方式来更新电子纸100上的显示画面。举例而言，当电子纸100具有多个显示屏幕时，服务装置10可更新多个显示屏幕中的部分或全部所显示的认证信息。或者，在电子纸100具有可局部更新的画面的功能的情况下，服务装置100亦可更新电子纸100上显示密码的特定区域，而不更新电子纸100的其他区域。

[0043] 图3中的步骤S32～S34当然也可应用于图4所绘示的认证方法中。详细而言，在步骤S41完成之后，使用者装置11可从电子纸100获得认证信息(步骤S32)，以及经由电性通道13传送帐号与密码给服务装置10以便登入服务装置10(步骤S33)。服务装置10的处理器101可以加密使用者装置11所传送来的密码而产生经加密数据，并检查所述经加密数据与非挥发性储存装置102中所储存的经加密密码是否一致(步骤S34)。

[0044] 图5为本发明另一实施例一认证方法的流程示意图。图5包括步骤S50～S55。整体而言，图5所绘示的认证方法可通过服务装置10于电子纸100上显示认证信息，让使用者装置11可检查服务装置10是否为合法装置。图5所示实施例将使用非对称加密演算法来进行认证操作。

[0045] 请参考图1与图5，在步骤S50中，使用者装置11可向服务装置10的处理器101请求建立通讯连接，并提供识别信息至服务装置10。依照设计需求，在一些实施例中，使用者装置11所提供的识别信息可以是与使用者装置11相关的识别信息。举例而言，与使用者装置11相关的所述识别信息可包括(例如但不限制于)使用者装置11的型号、用户识别模块(Subscriber Identity Module，SIM)卡数据、网络地址、使用者装置11发出请求的时间戳、

使用者装置11的定位位置、或者是其他关于使用者装置11端的信息。在另一些实施例中，使用者装置11所提供的识别信息可以是任何数据或数值。举例来说，使用者装置11所提供的识别信息可以包括伪随机(Pseudo-Random)值或是其他无关于使用者装置11的任何数据或数值。在将识别信息提供给服务装置10后，使用者装置11依然保留这个识别信息以便于步骤S55使用。

[0046] 在步骤S51中，服务装置10的处理器101以服务装置10的私钥(private key)加密使用者装置11所提供的识别信息，以产生经加密信息。详细而言，服务装置10的处理器101可以利用非对称加密演算法产生互相对应的公钥及私钥，并以私钥对使用者装置11所提供的识别信息进行加密。

[0047] 在步骤S52中，服务装置10的处理器101可将认证信息显示于电子纸100上。在本实施例中，显示于电子纸100的认证信息可以包括所述经加密信息以及服务装置10的公钥。图5所示步骤S52可以参照图2所示步骤S20的相关说明而将认证信息显示于电子纸100，故不再赘述。

[0048] 在步骤S53中，使用者装置11可从电子纸100获取认证信息(包括所述经加密信息以及服务装置10的公钥)。图5所示步骤S53可以参照图2所示步骤S21的相关说明，使得使用者装置11可通过适合的方式来获得显示在电子纸100上的认证信息，故不再赘述步骤S53的细节。

[0049] 在步骤S54中，使用者装置11可以利用服务装置10的公钥解密所述经加密信息，以产生经解密信息。由于所述经加密信息是服务装置10以私钥进行加密所产生的，故使用者装置11使用服务装置10的公钥应可正确解密所述经加密信息。

[0050] 在步骤S55中，使用者装置11可以检查所述经解密信息。如前述关于步骤S50的说明，在将识别信息提供给服务装置10后，使用者装置11依然保留这个识别信息。当所述经解密信息(所述经加密信息的解密结果)与这个识别信息一致时，则使用者装置11可以判定为“认证成功”(亦即服务装置10为合法装置)。反之，当所述经解密信息(所述经加密信息的解密结果)与这个识别信息不一致时，则使用者装置11可以判定为“认证失败”(亦即服务装置10为非法装置)。

[0051] 简言之，在图5绘示的认证方法中，使用者装置11可通过以服务装置10的公钥解密经使用者装置11加密的信息来判断公钥是否正确(密钥认证操作)。服务装置10的电子纸100通过非电性通道12提供服务装置10的公钥及经加密信息给使用者装置11。图5所绘示的认证方法可以避免黑客以钓鱼网站的认证接口来窃取使用者装置11的信息。此外，电子纸100所提供的非电性通道12还可以避免服务装置10的公钥在网络传输的过程中被窃取。因此，图5所绘示的认证方法可以有效避免钓鱼网站窃取数据或是认证信息的外流，进而有效改善认证系统1的信息安全。

[0052] 图6为本发明另一实施例一认证方法的流程示意图。图6所绘示的认证方法包括步骤S60～S67。整体而言，图6所绘示的认证方法可通过服务装置10于电子纸100上显示认证信息，让使用者装置11依据认证信息回复服务装置10。服务装置10可依据使用者装置11的回复内容检查使用者装置11是否为合法装置。图6所示实施例将使用非对称加密演算法来进行认证操作。

[0053] 请参考图1与图6，在步骤S60中，使用者装置11可向服务装置10的处理器101请求

建立通讯连接。响应于使用者装置11的请求，在步骤S61中，服务装置10的处理器101可产生识别信息。依照设计需求，在一些实施例中，服务装置10所提供的识别信息可以是与服务装置10相关的识别信息。举例而言，与服务装置10相关的所述识别信息可包括(例如但不限制于)服务装置10的系统信息、系统名称、系统时间、系统的网络地址等，或者是其他关于服务装置10的信息。在另一些实施例中，服务装置10所提供的识别信息可以是任何数据或数值。举例来说，服务装置10所提供的识别信息可以包括伪随机(Pseudo-Random)值或是其他无关于服务装置10的任何数据或数值。服务装置10可以保留这个识别信息，以便于步骤S67使用。

[0054] 在步骤S62中，服务装置10的处理器101可将认证信息显示于电子纸100上。在本实施例中，显示于电子纸100的认证信息包括所述识别信息以及服务装置10的公钥。图6所示步骤S62可以参照图2所示步骤S20的相关说明而将认证信息显示于电子纸100，故不再赘述。详细而言，服务装置10的处理器101可以利用非对称加密演算法产生互相对应的公钥及私钥，并将所述公钥以及所述识别信息显示于电子纸100上。

[0055] 在步骤S63中，使用者装置11可从电子纸100获取认证信息(包括所述识别信息以及服务装置10的公钥)。图6所示步骤S63可以参照图2所示步骤S21的相关说明，使得使用者装置11可通过适合的方式来获得显示在电子纸100上的认证信息，故不再赘述步骤S63的细节。

[0056] 在步骤S64中，使用者装置11可以使用服务装置10的公钥加密所述识别信息，以产生经加密信息。在步骤S65中，使用者装置11可以通过电性通道13(例如网际网络、区域网络以及/或是其他网络)提供经加密信息至服务装置10的处理器101，以便进行认证。由于服务装置10的公钥是通过非电性通道12传输给使用者装置11，故服务装置10的公钥信息安全无虞。使用者装置11使用服务装置10的公钥对服务装置10所提供的识别信息进行加密，可产生出黑客无法伪造的经加密信息。

[0057] 在步骤S66中，服务装置10的处理器101可以使用服务装置10的私钥解密所述经加密信息，以产生经解密信息。由于所述经加密信息是使用者装置11以服务装置10的公钥进行加密所产生的，故服务装置10使用服务装置10的私钥应可正确解密所述经加密信息。

[0058] 在步骤S67中，服务装置10的处理器101可以检查所述经解密信息。如前述关于步骤S61的说明，服务装置10保留这个识别信息，以便于步骤S67使用。当所述经解密信息(所述经加密信息的解密结果)与这个识别信息一致时，则处理器101可以判定为“认证成功”(亦即使用者装置11为合法装置)。反之，当所述经解密信息(所述经加密信息的解密结果)与这个识别信息不一致时，则处理器101可以判定为“认证失败”(亦即使用者装置11为非法装置)。

[0059] 简言之，在图6绘示的认证方法中，使用者装置11可通过服务装置10的公钥对服务装置10所提供的识别信息进行加密，并将加密结果(经加密信息)回传给服务装置10。服务装置10对经加密信息进行解密，以判断使用者装置11是否为合法装置。服务装置10的电子纸100通过非电性通道12提供认证信息(识别信息与服务装置10的公钥)给使用者装置11。图6所绘示的认证方法可有效避免黑客截取公钥与伪造公钥，故图6所绘示的认证方法可以有效改善认证系统1的信息安全。

[0060] 图7为本发明另一实施例一认证方法的流程示意图。图7所绘示的认证方法包括步

骤S70～S79。整体而言，图7所绘示的认证方法可以进行使用装置11以及服务装置10之间的双向认证。亦即，基于服务装置10的电子纸100所显示的认证信息，使用者装置11可以检查服务装置10是否为合法装置，而服务装置10亦可以检查使用者装置11是否为合法装置。

[0061] 请参考图1与图7，在步骤S70中，使用者装置11可向服务装置10的处理器101请求建立通讯连接，并提供第一识别信息至服务装置10。图7所示步骤S70可以参照图5所示步骤S50的相关说明，而步骤S70所述第一识别信息可以参照步骤S50所述识别信息的相关说明，故在此不予赘述。在将第一识别信息提供给服务装置10后，使用者装置11依然保留这个第一识别信息以便于步骤S75使用。

[0062] 在步骤S71中，服务装置10的处理器101可以使用服务装置10的私钥加密使用者装置11所提供的第一识别信息，以产生第一经加密信息。服务装置10的处理器101在步骤S71中还可以产生第二识别信息。服务装置10可以保留这个第二识别信息，以便于步骤S79使用。图7所示步骤S71可以参照图5所示步骤S51与/或图6所示步骤S61的相关说明，步骤S71所述第一识别信息与第一经加密信息可以参照步骤S51所述识别信息与经加密信息的相关说明，而步骤S71所述第二识别信息可以参照步骤S61所述识别信息的相关说明，故在此不予赘述。

[0063] 在步骤S72中，服务装置10的处理器101可将认证信息显示于电子纸100上。在本实施例中，显示于电子纸100的认证信息可包括服务装置10的公钥、所述第一经加密信息及所述第二识别信息。图7所示步骤S72可以参照图5所示步骤S52与/或图6所示步骤S62的相关说明，步骤S72所述第一经加密信息可以参照步骤S52所述经加密信息的相关说明，而步骤S72所述第二识别信息可以参照步骤S62所述识别信息的相关说明，故在此不予赘述。

[0064] 在步骤S73中，使用者装置11可从电子纸100获取认证信息(包括所述第一经加密信息、所述第二识别信息以及服务装置10的所述公钥)。图7所示步骤S73可以参照图2所示步骤S21的相关说明，使得使用者装置11可通过适合的方式来获得显示在电子纸100上的认证信息。图7所示步骤S73可以参照图5所示步骤S53与/或图6所示步骤S63的相关说明，步骤S73所述第一经加密信息可以参照步骤S53所述经加密信息的相关说明，而步骤S73所述第二识别信息可以参照步骤S63所述识别信息的相关说明，故在此不予赘述。

[0065] 在步骤S74中，使用者装置11可以利用服务装置10的公钥解密所述第一经加密信息，以产生第一经解密信息。图7所示步骤S74可以参照图5所示步骤S54的相关说明，步骤S74所述第一经加密信息与第一经解密信息可以参照步骤S54所述经加密信息与经解密信息的相关说明，故在此不予赘述。

[0066] 在步骤S75中，使用者装置11可以检查所述第一经解密信息。在步骤S70将第一识别信息提供给服务装置10后，使用者装置11依然保留这个第一识别信息。当所述第一经解密信息(所述第一经加密信息的解密结果)与这个第一识别信息一致时，则使用者装置11可以判定为“认证成功”(亦即使用者装置11判定服务装置10为合法装置)。反之，当所述第一经解密信息(所述第一经加密信息的解密结果)与这个第一识别信息不一致时，则使用者装置11可以判定为“认证失败”(亦即使用者装置11判定服务装置10为非法装置)。图7所示步骤S75可以参照图5所示步骤S55的相关说明，步骤S75所述第一识别信息与第一经解密信息可以参照步骤S55所述识别信息与经解密信息的相关说明，故在此不予赘述。

[0067] 在步骤S76中，使用者装置11可以使用服务装置10的公钥加密所述第二识别信息，

以产生第二经加密信息。图7所示步骤S76可以参照图6所示步骤S64的相关说明，步骤S76所述第二识别信息与第二经加密信息可以参照步骤S64所述识别信息与经加密信息的相关说明，故在此不予赘述。

[0068] 在步骤S77中，使用者装置11可以通过电性通道13(例如网际网络、区域网络以及/或是其他网络)提供所述第二经加密信息至服务装置10的处理器101，以便进行认证。图7所示步骤S77可以参照图6所示步骤S65的相关说明，步骤S77所述第二经加密信息可以参照步骤S65所述经加密信息的相关说明，故在此不予赘述。

[0069] 在步骤S78中，服务装置10的处理器101可以使用服务装置10的私钥解密所述第二经加密信息，以产生第二经解密信息。图7所示步骤S78可以参照图6所示步骤S66的相关说明，步骤S78所述第二经加密信息与第二经解密信息可以参照步骤S66所述经加密信息与经解密信息的相关说明，故在此不予赘述。

[0070] 在步骤S79中，服务装置10的处理器101可以检查所述第二经解密信息。如前述关于步骤S71的说明，服务装置10保留了这个第二识别信息，以便于步骤S79使用。当所述第二经解密信息(所述第二经加密信息的解密结果)与这个第二识别信息一致时，则处理器101可以判定为“认证成功”(亦即服务装置10判定使用者装置11为合法装置)。反之，当所述第二经解密信息(所述第二经加密信息的解密结果)与这个第二识别信息不一致时，则处理器101可以判定为“认证失败”(亦即服务装置10判定使用者装置11为非法装置)。图7所示步骤S79可以参照图6所示步骤S67的相关说明，步骤S79所述第二经解密信息与第二识别信息可以参照步骤S67所述经解密信息与识别信息的相关说明，故在此不予赘述。

[0071] 如此一来，在服务装置10及使用者装置11双端都认证成功的情况下，服务装置10及使用者装置11之间的通讯连接可以被成功建立。

[0072] 综上所述，基于诸实施例所述认证方法，认证系统1的服务装置10可以使用电子纸100所提供的非电性通道12来取代电性通道13(例如网际网络、区域网络以及/或是其他网络)，以便传输认证信息。利用电子纸100所提供认证信息，使用者装置11可以进行认证操作。通过电子纸提供(传输)认证信息可有效避免认证信息被非法截取。故，上述诸实施例的认证方法及认证系统1可有效改善信息安全。

[0073] 以上所述仅为本发明较佳实施例，然其并非用以限定本发明的范围，任何熟悉本项技术的人员，在不脱离本发明的精神和范围内，可在此基础上做进一步的改进和变化，因此本发明的保护范围当以本申请的权利要求书所界定的范围为准。

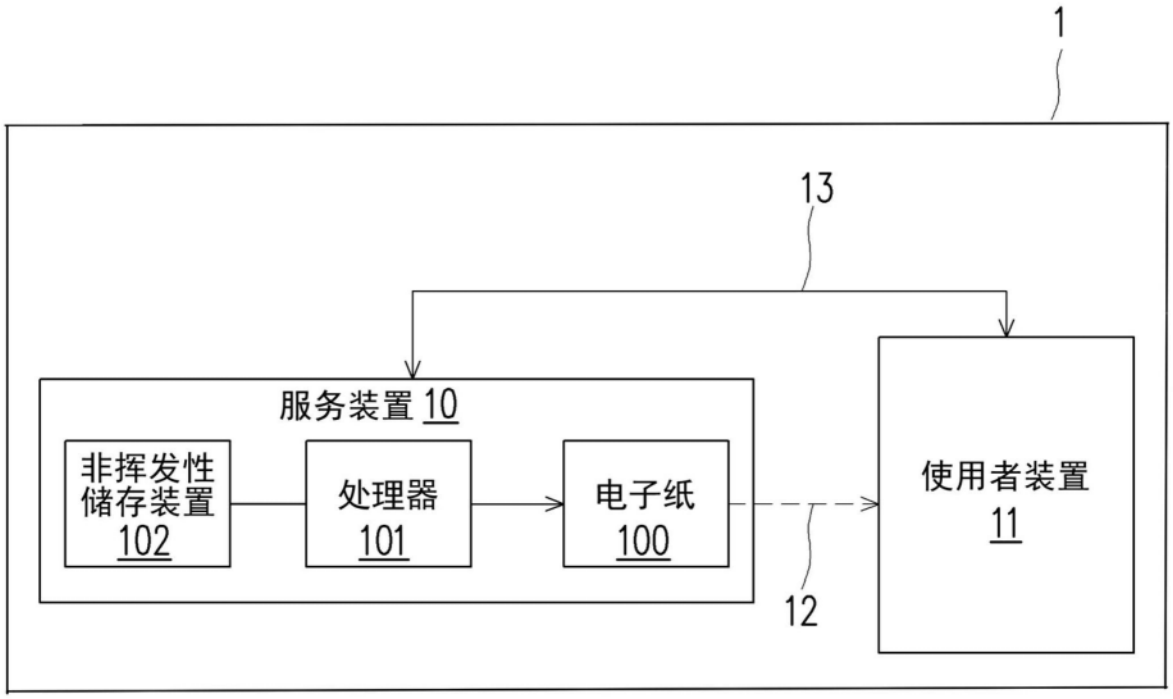

1
13
服务装置 10
非挥发性储存装置 102
处理器 101
电子纸 100
使用者装置 11
12

图1

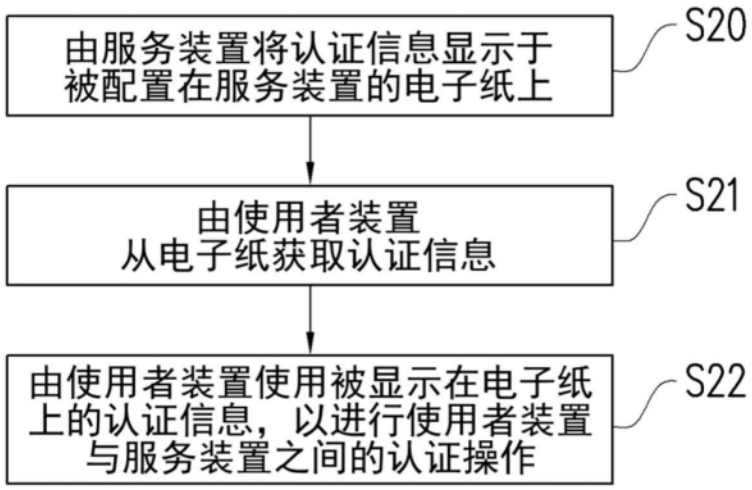

由服务装置将认证信息显示于被配置在服务装置的电子纸上
S20
由使用者装置从电子纸获取认证信息
S21
由使用者装置使用被显示在电子纸上的认证信息，以进行使用者装置与服务装置之间的认证操作
S22

图2

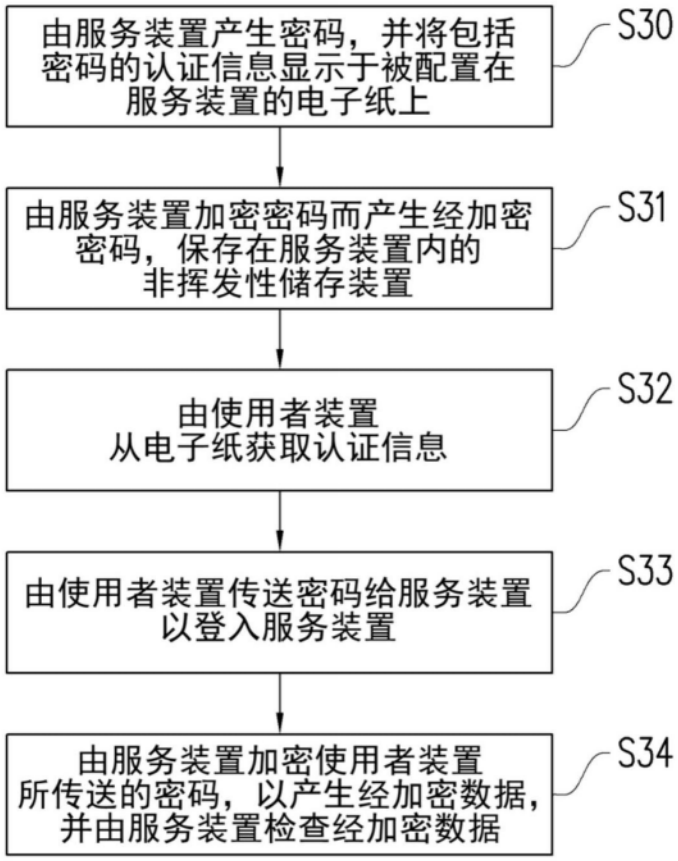

由服务装置产生密码，并将包括密码的认证信息显示于被配置在服务装置的电子纸上
S30
由服务装置加密密码而产生经加密密码，保存在服务装置内的非挥发性储存装置
S31
由使用者装置从电子纸获取认证信息
S32
由使用者装置传送密码给服务装置以登入服务装置
S33
由服务装置加密使用者装置所传送的密码，以产生经加密数据，并由服务装置检查经加密数据
S34

图3

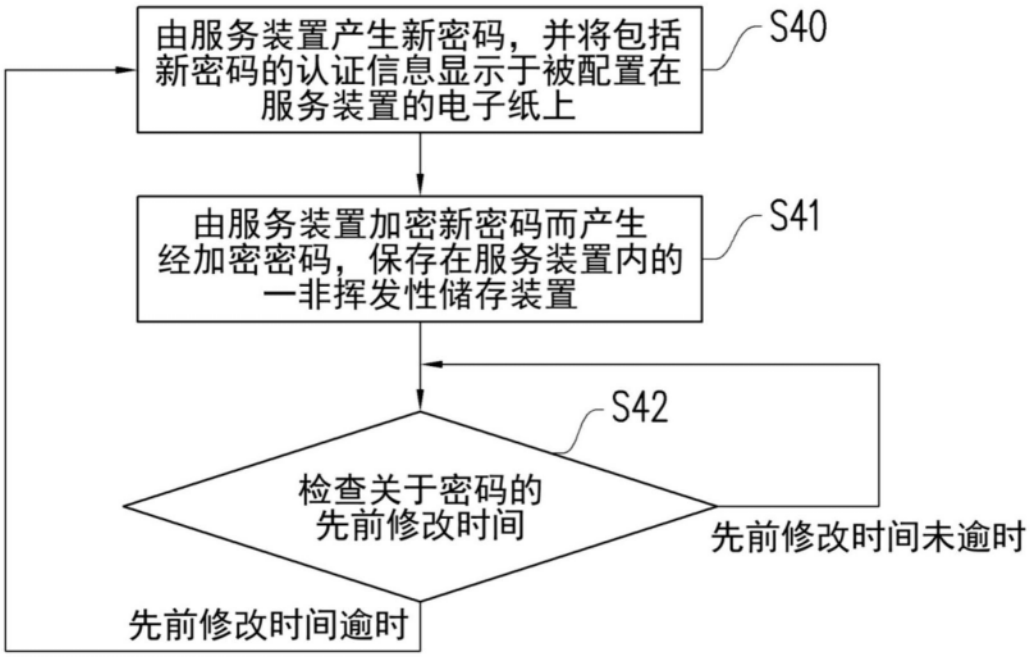

由服务装置产生新密码，并将包括新密码的认证信息显示于被配置在服务装置的电子纸上
S40
由服务装置加密新密码而产生经加密密码，保存在服务装置内的一非挥发性储存装置
S41
S42
检查关于密码的先前修改时间
先前修改时间未逾时
先前修改时间逾时

图4

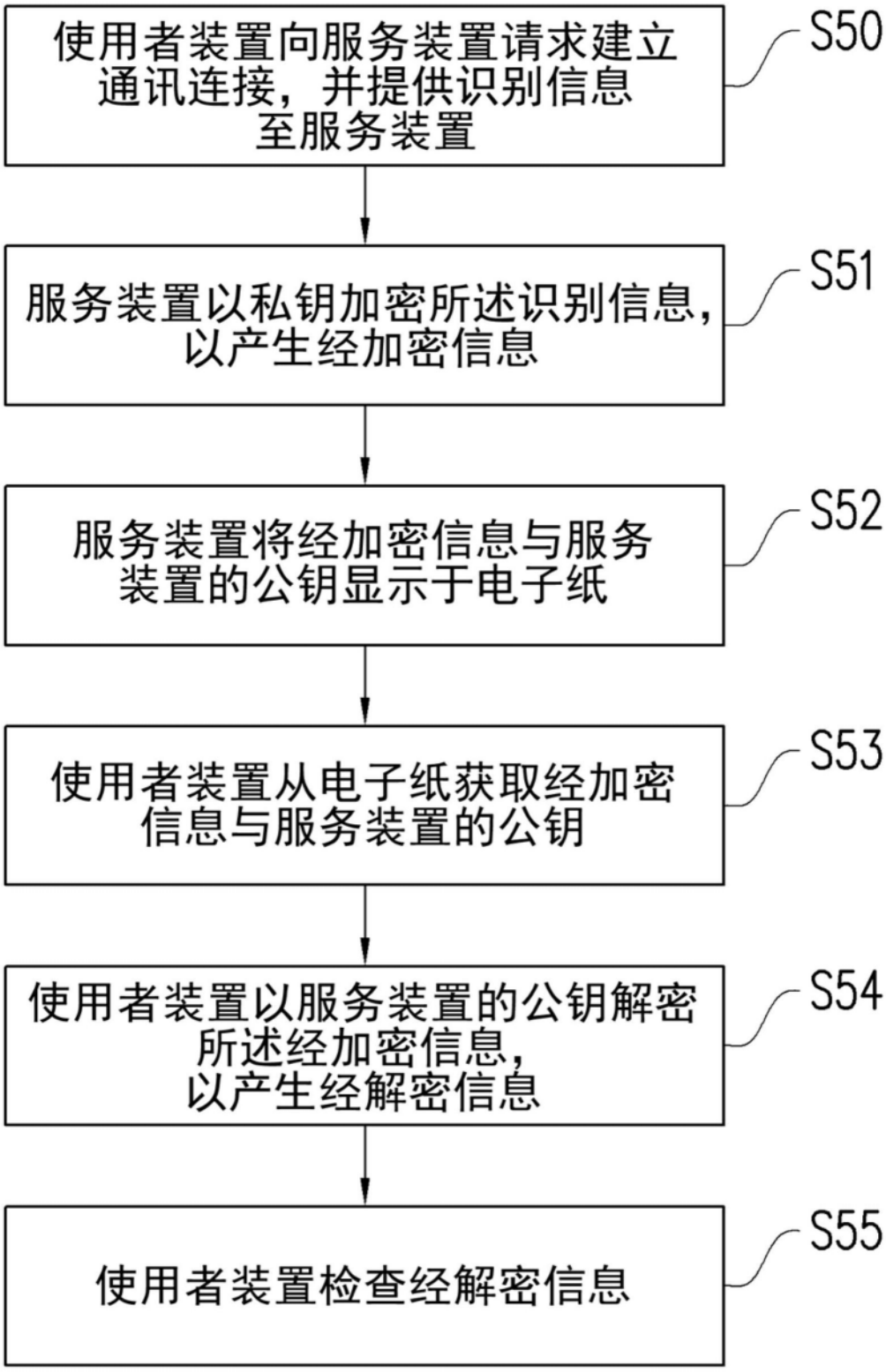

使用者装置向服务装置请求建立通讯连接，并提供识别信息至服务装置
S50
服务装置以私钥加密所述识别信息，以产生经加密信息
S51
服务装置将经加密信息与服务装置的公钥显示于电子纸
S52
使用者装置从电子纸获取经加密信息与服务装置的公钥
S53
使用者装置以服务装置的公钥解密所述经加密信息，以产生经解密信息
S54
使用者装置检查经解密信息
S55

图5

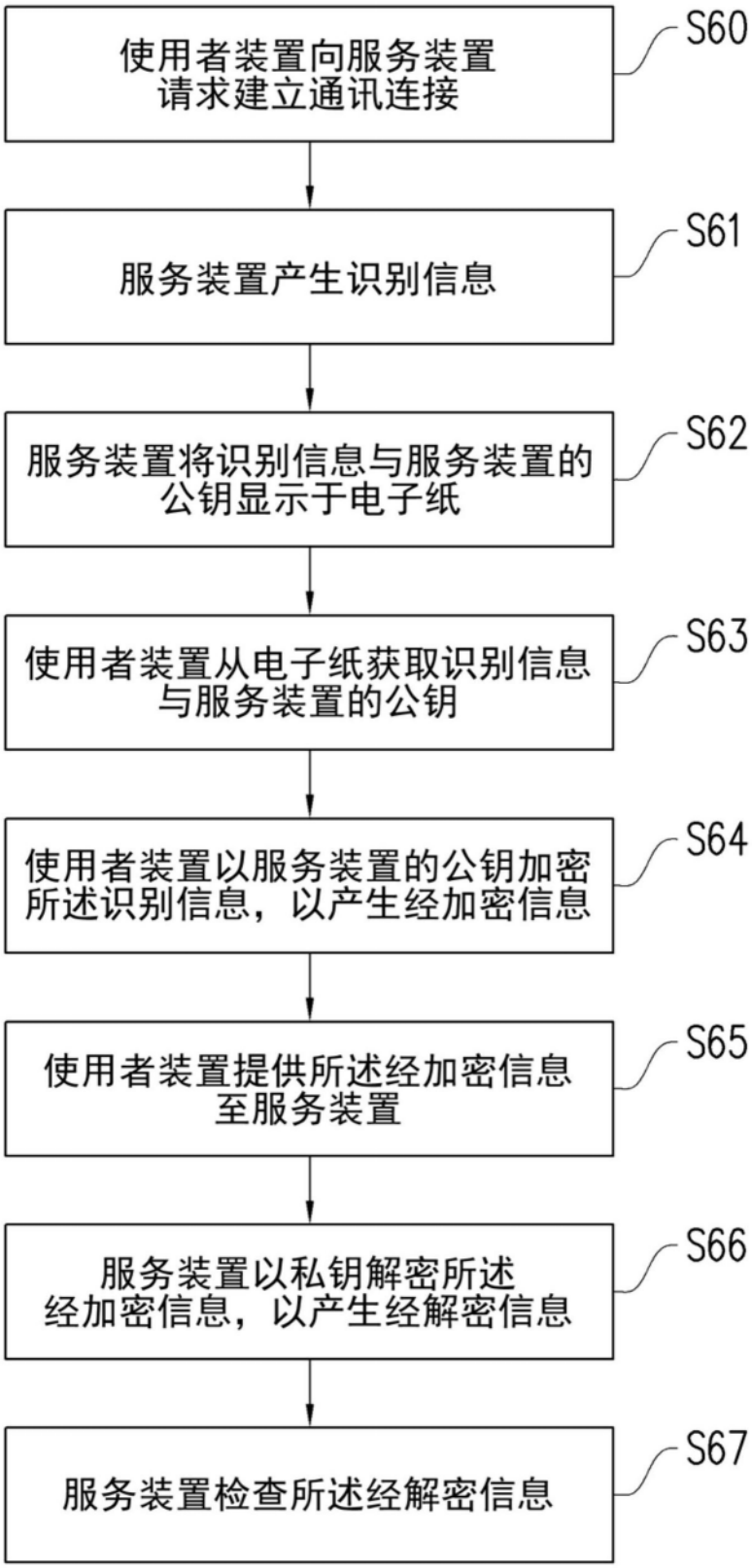

使用者装置向服务装置
请求建立通讯连接
S60
服务装置产生识别信息
S61
服务装置将识别信息与服务装置的
公钥显示于电子纸
S62
使用者装置从电子纸获取识别信息
与服务装置的公钥
S63
使用者装置以服务装置的公钥加密
所述识别信息，以产生经加密信息
S64
使用者装置提供所述经加密信息
至服务装置
S65
服务装置以私钥解密所述
经加密信息，以产生经解密信息
S66
服务装置检查所述经解密信息
S67

图6

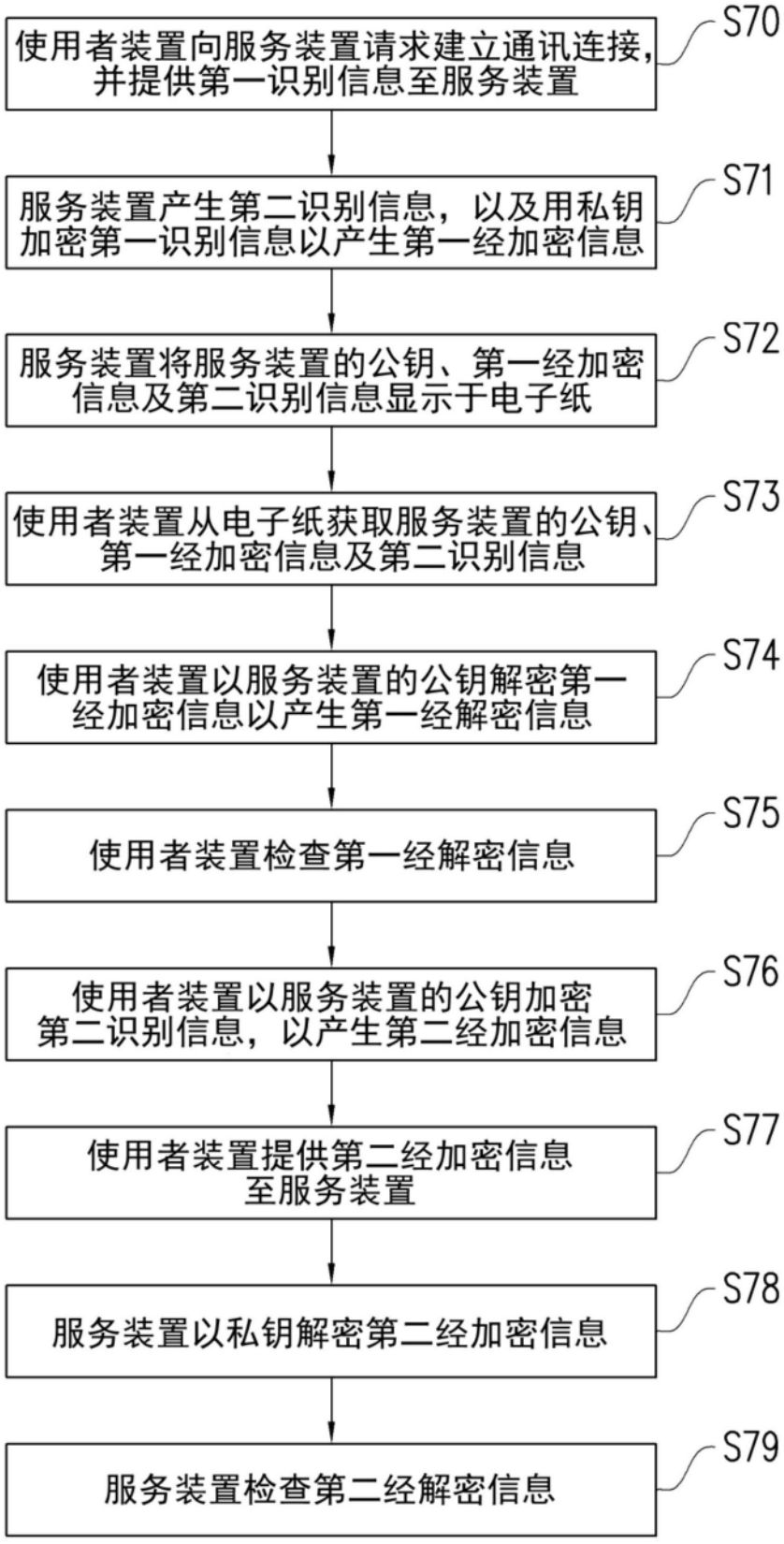

使用者装置向服务装置请求建立通讯连接，并提供第一识别信息至服务装置
S70
服务装置产生第二识别信息，以及用私钥加密第一识别信息以产生第一经加密信息
S71
服务装置将服务装置的公钥、第一经加密信息及第二识别信息显示于电子纸
S72
使用者装置从电子纸获取服务装置的公钥、第一经加密信息及第二识别信息
S73
使用者装置以服务装置的公钥解密第一经加密信息以产生第一经解密信息
S74
使用者装置检查第一经解密信息
S75
使用者装置以服务装置的公钥加密第二识别信息，以产生第二经加密信息
S76
使用者装置提供第二经加密信息至服务装置
S77
服务装置以私钥解密第二经加密信息
S78
服务装置检查第二经解密信息
S79

图7