[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 9/32 (2006.01)
H04L 29/06 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200810180541.1

[43] 公开日 2009 年 4 月 29 日

[11] 公开号 CN 101420302A

[22] 申请日 2008.12.1
[21] 申请号 200810180541.1
[71] 申请人 成都市华为赛门铁克科技有限公司
地址 611731 四川省成都市高新区西部园区清水河片区
[72] 发明人 万峪臣

[74] 专利代理机构 北京挺立专利事务所
代理人 叶树明

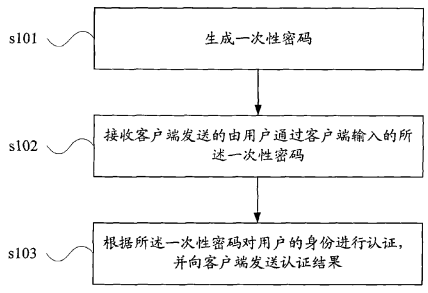
权利要求书 3 页 说明书 8 页 附图 4 页

[54] 发明名称

安全认证方法和设备

[57] 摘要

本发明公开了一种安全认证方法和安全认证设备。 该方法应用于在客户端和网络侧认证服务器之外的第三方认证设备上，所述第三方设备与所述客户端连接，包括：生成一次性密码；接收客户端发送的由用户通过所述客户端输入的一次性密码；根据所述一次性密码对所述用户的身份进行认证，并向所述客户端发送认证结果。 本发明的实施例中，将一次性密码的生成以及对用户输入的一次性密码的认证在服务器外的安全认证设备上进行，使得非法用户无法通过破解服务器的认证算法或盗取用户密码的方式威胁正常用户的使用，保证了服务器和用户的数据安全。



1、一种安全认证方法，应用于在客户端和网络侧认证服务器之外的第三方认证设备上，所述第三方设备与所述客户端连接，其特征在于，包括:

生成一次性密码;

接收所述客户端发送的由用户通过所述客户端输入的所述一次性密码;

根据输入的所述一次性密码对所述用户的身份进行认证，并向所述客户端发送认证结果。

2、如权利要求 1 所述的方法，其特征在于，所述生成一次性密码包括:

接收用户输入的口令;

所述口令正确时，根据预设的动态参数生成一次性密码。

3、如权利要求 1 所述的方法，其特征在于，所述生成一次性密码后，还包括:

将所述一次性密码通过所述第三方设备显示；或将所述密码通过所述客户端显示。

4、如权利要求 1 或 2 所述的方法，其特征在于，所述根据输入的一次性密码对所述用户的身份进行认证包括:

根据本地存储的最近一次使用的预设动态参数生成中间密码;

所述中间密码与输入的所述一次性密码相同时，判断对所述用户的身份认证通过；否则判断对所述用户的身份认证失败。

5、如权利要求 1 或 2 所述的方法，其特征在于，所述生成一次性密码后还包括：使用所述一次性密码对所述用户输入的口令进行加密，得到加密后的用户输入的口令;

所述根据输入的一次性密码对所述用户的身份进行认证包括：使用所述输入的一次性密码对所述加密后的用户输入的口令进行解密，当解密结果为所述用户输入的口令时，判断对所述用户的身份认证通过；否则判断对所述用户的身份认证失败。

6、如权利要求 4 所述的方法，其特征在于，所述动态参数包括当前时间、或使用次数、或随机数中的一种或多种。

7、如权利要求 1 或 2 所述的方法，其特征在于，所述向客户端发送认证

结果包括:

将所述认证结果进行加密并向所述客户端发送;

所述将所述认证结果进行加密并向所述客户端发送后还包括:

所述客户端将所述加密后的认证结果向所述网络侧认证服务器发送，触发所述网络侧认证服务器根据解密得到的所述认证结果进行操作。

8、如权利要求 1 或 2 所述的方法，其特征在于，所述向所述客户端发送认证结果后，还包括:

所述客户端将所述认证结果进行加密后向所述网络侧认证服务器发送，触发所述网络侧认证服务器根据解密得到的所述认证结果进行操作。

9、一种安全认证设备，其特征在于，作为客户端和网络侧认证服务器之外的第三方认证设备并与所述客户端连接，包括:

密码生成单元，用于生成一次性密码;

客户端接口单元，用于接收所述客户端发送的由用户通过所述客户端输入的所述一次性密码;

密码认证单元，用于根据输入的所述一次性密码对所述用户的身份进行认证，并向所述客户端发送认证结果。

10、如权利要求 9 所述的安全认证设备，其特征在于，还包括:

密码显示单元，用于显示所述密码生成单元生成的所述一次性密码。

11、如权利要求 9 所述的安全认证设备，其特征在于，所述密码生成单元包括:

口令输入子单元，用于接收用户输入的口令;

口令验证子单元，用于在所述口令输入子单元接收的口令正确时，根据预设的动态参数生成一次性密码。

12、如权利要求 11 所述的安全认证设备，其特征在于，所述密码认证单元包括第一密码认证子单元，用于: 根据本地存储的最近一次使用的动态参数生成中间密码; 所述中间密码与所述输入的一次性密码相同时，判断对所述用户的身份认证通过; 否则判断对所述用户的身份认证失败。

13、如权利要求 11 所述的安全认证设备，其特征在于，所述密码认证单

元包括第二密码认证子单元，用于：使用所述密码生成单元生成的一次性密码对所述用户输入的口令进行加密，得到加密后的用户输入的口令；使用所述客户端接口单元接收到的所述输入的一次性密码对所述加密后的用户输入的口令进行解密，当解密结果为所述用户输入的口令时，判断对所述用户的身份认证通过；否则判断对所述用户的身份认证失败。

14、如权利要求 12 或 13 所述的安全认证设备，其特征在于，所述密码认证单元还包括：

认证结果加密子单元，用于将所述认证结果进行加密后向所述客户端发送。

15、如权利要求 9 或 10 或 11 所述的安全认证设备，其特征在于，所述密码生成单元和密码认证单元位于所述安全认证设备的 USBKEY 功能芯片上。

安全认证方法和设备

技术领域

本发明涉及通信技术领域，特别涉及一种安全认证方法和设备。

背景技术

随着计算机技术日新月异的发展，网络安全面临着很大的挑战，尤其是网上银行服务器、电子商务网站等要求安全性极高的系统，往往是黑客们攻击的重中之重。现有技术中，通过动态密码锁，合法客户们能够较为安全的登录使用涉及金额操作的服务器系统。

动态密码锁也称一次性密码，其内置电源、密码生成芯片和显示屏。数字键用于输入用户 PIN（Personal Identification Number，个人识别码）码，芯片运行专门的密码算法，生成当前密码并显示在显示屏上。用户每次输入正确的 PIN 码后都可以得到一个一次性动态密码，认证服务器采用相同的算法计算当前的有效密码。由于只有合法用户才持有该硬件，所以只要一次性密码验证通过，系统就可以认为该用户的身份可靠。由于用户每次登录必须使用另外一个动态密码，因此即使黑客截获了一次密码，也无法利用这个密码来仿冒合法用户的身份。

在实现本发明的过程中，发明人发现现有技术至少存在以下问题:

对于动态密码锁，在服务器端的认证系统里可以计算出所有动态密码，一旦银行认证服务器系统被破解就会对银行系统造成很大安全威胁，另外网银的管理员可以在服务器端人为的修改动态密码锁的规则，因此具有一定的安全隐患。

发明内容

本发明实施例提供一种安全认证方法和设备，用于保证服务器和客户端的数据安全。

本发明实施例提供一种安全认证方法，应用于在客户端和网络侧认证服务器之外的第三方认证设备上，所述第三方设备与所述客户端连接，包括：

生成一次性密码；

接收所述客户端发送的由用户通过所述客户端输入的所述一次性密码；

根据输入的所述一次性密码对所述用户的身份进行认证，并向所述客户端发送认证结果。

本发明实施例还提供一种安全认证设备，作为客户端和网络侧认证服务器之外的第三方认证设备并与所述客户端连接，包括：

密码生成单元，用于生成一次性密码；

客户端接口单元，用于接收所述客户端发送的由用户通过所述客户端输入的所述一次性密码；

密码认证单元，用于根据输入的所述一次性密码对所述用户的身份进行认证，并向所述客户端发送认证结果。

与现有技术相比，本发明实施例具有以下优点：

本发明的实施例中，将对用户输入的一次性密码的认证在服务器外的安全认证设备上进行，使得非法用户无法通过破解服务器的认证算法或盗取用户密码的方式威胁正常用户的使用，保证了服务器和用户的数据安全。

附图说明

为了更清楚地说明本发明实施例的技术方案，下面将对实施例描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

图 1 是本发明实施例中安全认证方法的流程图；

图 2 是本发明实施例中一次性密码的生成流程图；

图 3 是本发明实施例中根据一次性密码进行认证的流程图；

图 4 是本发明实施例中安全认证设备的结构示意图；

图 5 是本发明实施例中安全认证设备的另一结构示意图。

具体实施方式

下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本发明的一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

本发明实施例提供一种安全认证方法，应用于在客户端和网络侧认证服务器之外的第三方认证设备上，该第三方设备与客户端连接，如图1所示，包括:

步骤 s101、生成一次性密码。

步骤 s102、接收客户端发送的由用户通过客户端输入的一次性密码。

步骤 s103、根据一次性密码对用户的身份进行认证，并向客户端发送认证结果。

本发明的实施例中，将一次性密码的生成以及对用户输入的一次性密码的认证在服务器外的安全认证设备上进行，使得非法用户无法通过破解服务器的认证算法或盗取用户密码的方式威胁正常用户的使用，保证了服务器和用户的数据安全。

本发明实施例提供一种安全认证方法，其包括根据用户输入的 PIN 码生成密码、以及对用户输入的密码进行认证两部分流程。以下分别对两部分流程进行描述。

本发明实施例提供的安全认证方法中，根据用户输入的 PIN 码生成密码的流程如图 2 所示，包括:

步骤 s201、接收用户输入的 PIN 码。

具体的，应用本发明实施例提供的全认证方法的安全认证设备上，具有输入装置如键盘，用户可以通过该输入装置输入 PIN 码。该 PIN 码是用户预先可以获知的，是使用该安全认证设备的基本条件。

步骤 s202、对用户输入的 PIN 码进行认证。

具体的，根据本地预先设置的正确 PIN 码，对用户输入的 PIN 码进行认证。当然，也可以采用其它认证方式，本发明实施例对此不做限定。

步骤 s203、对用户输入的 PIN 码认证通过时，生成一次性密码。

具体的，对用户输入的 PIN 码认证通过时，根据预设的动态参数生成一次性密码，可以使用的动态参数包括当前时间、安全认证设备使用次数、随机数中的一种或多种。对于生成一次性密码所采用的算法，可以使用 PKI（Public Key Infrastructure，公开密钥基础设施）标准对称或非对称算法，本发明实施例不做限定。另外，对 PIN 码的认证失败时，可以向用户进行提示或不进行任何处理，本发明的实施例对此不进行详细描述。

步骤 s204、显示该生成的一次性密码。

具体的，应用本发明实施例提供的全认证方法的安全认证设备上，具有显示装置如 LED（Light Emitting Diode，发光二极管）显示屏，通过该显示装置将生成的一次性密码显示给用户。该步骤 s204 为可选步骤，该一次性密码也可以通过与安全认证设备连接的客户端显示给用户。

本发明实施例提供的安全认证方法中，对用户输入的密码进行认证的流程如图 3 所示，包括:

步骤 s301、用户通过客户端程序输入其认为正确的一次性密码。

具体的，该客户端程序可以包括运行于服务器上用于登录特定服务如网上银行、商务网站等的程序，通过该客户端程序的界面，用户输入其认为正确的一次性密码。

步骤 s302、接收客户端程序发送的由用户输入的一次性密码。

具体的，用户在通过客户端程序进行登录时，为了确保登录成功，需要将应用本发明实施例安全认证方法的安全认证设备与客户端连接（如通过 USB 接口）。客户端程序接收到用户输入的一次性密码后，将该一次性密码向本发明实施例的安全认证设备发送

步骤 s303、对该一次性密码进行认证。

具体的，对该一次性密码进行认证的方法可以有很多，本发明的实施例

列举以下两种：

（1）在前述步骤 s203 中根据预设的动态参数生成一次性密码时，将生成一次性密码所使用的动态参数进行存储。本步骤中需要对用户输入的一次性密码进行认证时，首先根据本地存储的最近一次使用的动态参数生成一个中间密码；之后将该中间密码与用户输入的一次性密码进行比较，比较结果为相同时，判断对该一次性密码也即用户身份的认证通过；否则判断对该一次性密码也即用户身份的认证失败。

（2）在前述步骤 s203 中根据预设的动态参数生成一次性密码后，使用该一次性密码对特定内容（如用户的 PIN 码）进行加密，加密所使用的算法不限。当接收到用户输入的一次性密码时，使用该用户输入的一次性密码对上述加密后的特定内容（如用户的 PIN 码）进行解密，当解密结果为正确的特定内容（如用户的 PIN 码）时，判断对该一次性密码也即用户身份的认证通过；否则判断对该一次性密码也即用户身份的认证失败。

步骤 s304、向客户端程序发送认证结果。

具体的，认证结果为通过时，客户端程序连接到特定服务供用户使用；否则可以向用户进行提示或不进行任何处理，本发明的实施例对此不进行详细描述。另外，为了保证上述“一次性密码”只能使用一次，向客户端程序发送认证通过结果后，丢弃与该一次性密码相关的内容，使得用户在下次认证时，即使输入上一次通过认证所使用的密码仍无法通过认证。

步骤 s305、客户端将认证结果向网络侧认证服务器发送，触发网络侧认证服务器根据认证结果进行操作。

另外，上述步骤 s304 中，可以在向客户端程序发送认证结果前先对认证结果进行加密，之后再向客户端发送；或在步骤 s304 中不加密，而在步骤 s305 中由客户端对认证结果进行加密。无论采用哪种方法，客户端都是将加密后的认证结果向网络侧认证服务器发送，触发网络侧认证服务器根据解密得到的认证结果进行操作。具体的，步骤 s304 或步骤 s305 中的加密方法与网络侧认证服务器使用的解密方法相对应，可采用的加密/解密算法包括 AES（Advanced Encryption Standard，高级加密标准）算法但不限于 AES 算法。

通过该加密/解密处理，保护了认证结果在网络中的传输安全。

现有技术中除了动态密码锁技术外，还提供了 USBKEY 技术，USBKEY 是一种 USB（Universal Serial Bus，通用串行总线）接口的硬件设备，内置单片机或智能卡芯片，有一定的存储空间，可以存储用户的私钥以及数字证书，并利用 USBKEY 内置的公钥算法实现对用户身份的认证。而对于 USBKEY，由于 PIN 码非一次性密码，且是在客户端上输入并通过网络侧传递给认证服务器的，黑客可以通过木马程序截获用户 PIN 码并取得虚假认证，造成极大的安全隐患。相比较可以发现，本发明实施例中提供的方法同时兼具有现有技术 USBKEY 和动态密码锁中认证方法的优点，使用一次性密码，并将一次性密码的生成以及对用户输入的一次性密码的认证在服务器外的安全认证设备上进行，使得非法用户无法通过破解服务器的认证算法、或通过木马程序盗取在网络中传递的用户密码的方式威胁正常用户的使用，保证了服务器和用户的数据安全。

本发明的实施例还提供一种安全认证设备，作为客户端和网络侧认证服务器之外的第三方认证设备，并与客户端连接，如图 4 所示，包括：

密码生成单元 10，用于生成一次性密码。

具体的，可以根据预设的动态参数生成一次性密码，动态参数包括当前时间、安全认证设备使用次数、随机数中的一种或多种。

客户端接口单元 20，用于接收客户端发送的由用户通过客户端输入的一次性密码。具体的，用户在客户端程序输入一次性密码时，客户端程序将一次性密码发送到安全认证设备的客户端接口单元 20。

密码认证单元 30，用于根据客户端接口单元 20 接收的一次性密码对用户的身份进行认证，并向客户端发送认证结果。

本发明的另一实施例中，还提供了一种安全认证设备，作为客户端和网络侧认证服务器之外的第三方认证设备，并与客户端连接，如图 5 所示，还包括：

密码显示单元 40，用于显示密码生成单元 10 生成的一次性密码。

另外，上述密码生成单元 10 可以包括：

口令输入子单元 11，用于接收用户输入的口令。

口令验证子单元 12，用于在口令输入子单元 11 接收的口令正确时，根据预设的动态参数生成一次性密码。

另外，上述密码认证单元 30 可以包括:

第一密码认证子单元 31，用于：根据本地存储的最近一次使用的动态参数生成中间密码；该中间密码与上述输入的所述一次性密码相同时，判断对用户的身份认证通过；否则判断对用户的身份认证失败。

第二密码认证子单元 32，用于：使用密码生成单元 10 生成的一次性密码对用户输入的口令进行加密，得到加密后的用户输入的口令；使用客户端接口单元 20 接收到的由用户输入的一次性密码，对加密后的用户输入的口令进行解密，当解密结果为该用户输入的口令时，判断对用户的身份认证通过；否则判断对用户的身份认证失败。

为使本实施例方法的安全性进一步提高，可以在本装置向客户端程序发送认证结果前先对认证结果进行加密，因此，所述密码认证单元 30 还可以包括:

认证结果加密子单元 33，用于将认证结果进行加密后向客户端发送。由客户端将加密后的认证结果向网络侧认证服务器发送，触发网络侧认证服务器根据解密得到的所述认证结果进行操作。客户端将加密后的认证结果向网络侧认证服务器发送，触发网络侧认证服务器根据解密得到的认证结果进行操作。具体的，所使用的加密方法与网络侧认证服务器使用的解密方法相对应，可采用的加密/解密算法包括 AES（Advanced Encryption Standard，高级加密标准）算法但不限于 AES 算法。

另外，上述密码生成单元 10 和密码认证单元 30 可以位于安全认证设备的 USBKEY 功能芯片上；上述口令输入子单元 11 可以为键盘；上述密码显示单元 40 可以为 LED 显示装置。

本发明的实施例中，将一次性密码的生成以及对用户输入的一次性密码的认证在服务器外的安全认证设备上进行，使得非法用户无法通过破解服务器的认证算法、或通过客户端木马程序盗取密码的方式威胁正常用户的使用，

保证了服务器和用户的数据安全。另外，同时兼具有 USBKEY 和动态密码锁的优点。

上述模块可以分布于一个装置，也可以分布于多个装置。上述模块可以合并为一个模块，也可以进一步拆分成多个子模块。

通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到本发明可以通过硬件实现，也可以借助软件加必要的通用硬件平台的方式来实现。基于这样的理解，本发明的技术方案可以以软件产品的形式体现出来，该软件产品可以存储在一个非易失性存储介质（可以是 CD-ROM，U 盘，移动硬盘等）中，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备等）执行本发明各个实施例所述的方法。

本领域技术人员可以理解附图只是一个优选实施例的示意图，附图中的模块或流程并不一定是实施本发明所必须的。

本领域技术人员可以理解实施例中的装置中的模块可以按照实施例描述进行分布于实施例的装置中，也可以进行相应变化位于不同于本实施例的一个或多个装置中。上述实施例的模块可以合并为一个模块，也可以进一步拆分成多个子模块。

上述本发明实施例序号仅仅为了描述，不代表实施例的优劣。

以上公开的仅为本发明的几个具体实施例，但是，本发明并非局限于此，任何本领域的技术人员能思之的变化都应落入本发明的保护范围。

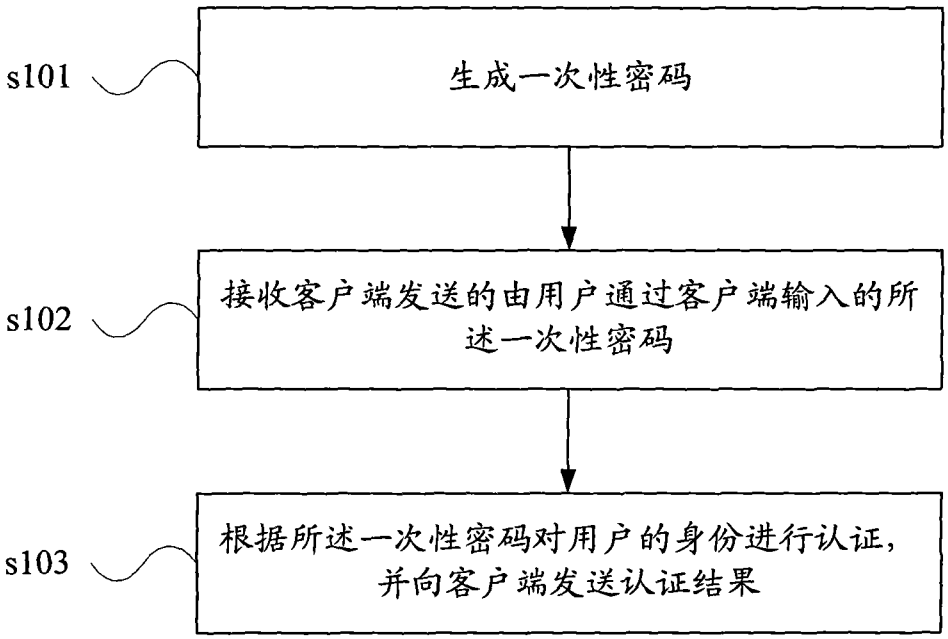

s101
生成一次性密码
s102
接收客户端发送的由用户通过客户端输入的所述一次性密码
s103
根据所述一次性密码对用户的身份进行认证，并向客户端发送认证结果

图 1

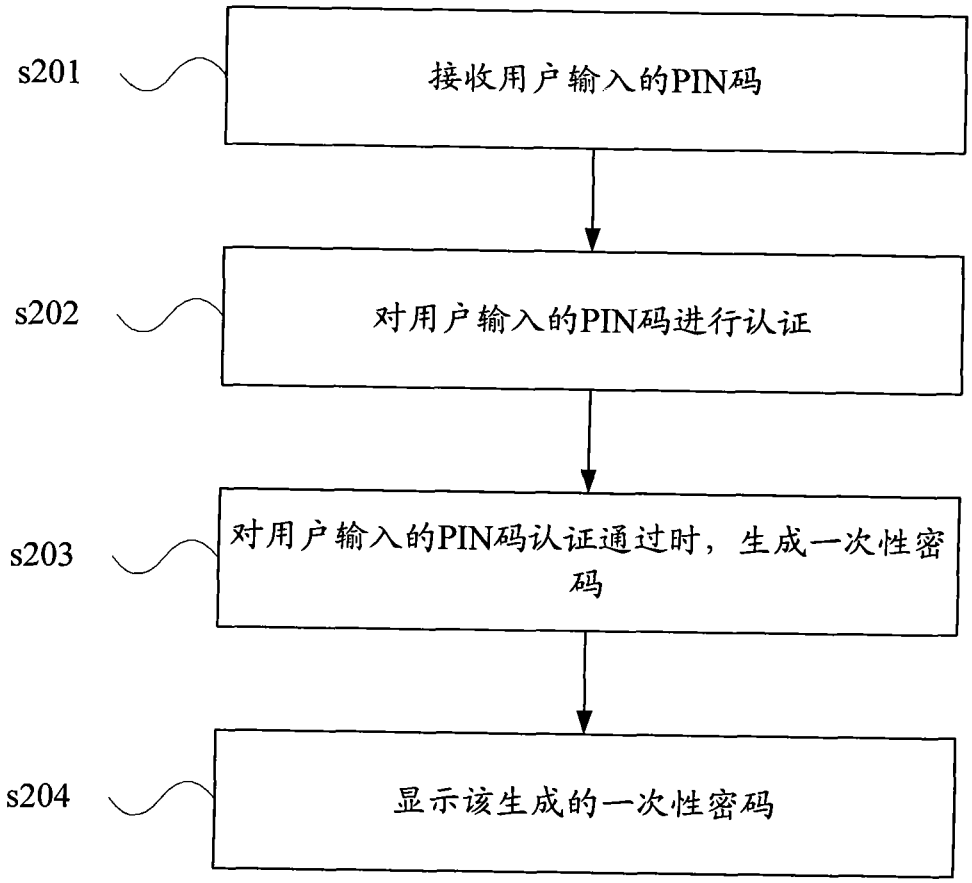

s201
接收用户输入的PIN码
s202
对用户输入的PIN码进行认证
s203
对用户输入的PIN码认证通过时，生成一次性密码
s204
显示该生成的一次性密码

图 2

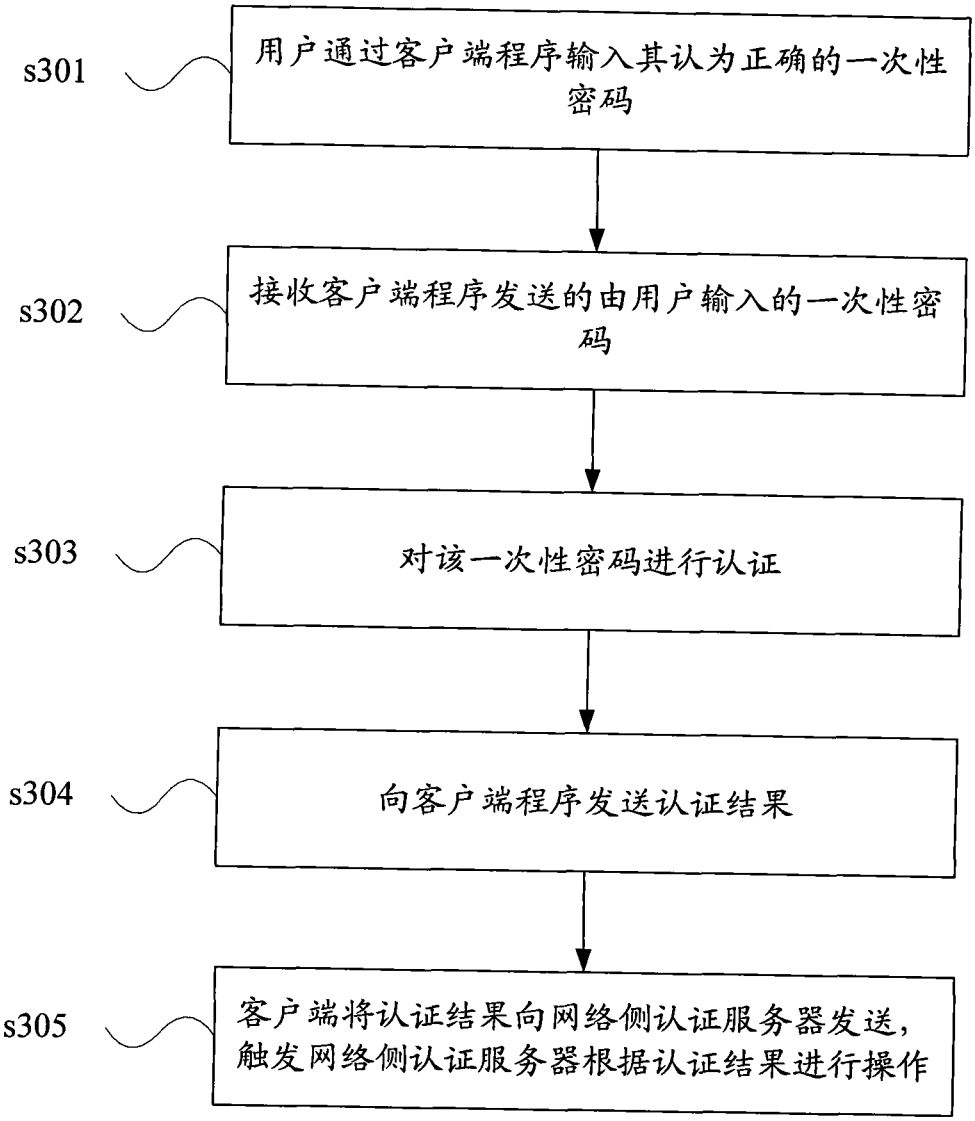

s301
用户通过客户端程序输入其认为正确的一次性密码
s302
接收客户端程序发送的由用户输入的一次性密码
s303
对该一次性密码进行认证
s304
向客户端程序发送认证结果
s305
客户端将认证结果向网络侧认证服务器发送，触发网络侧认证服务器根据认证结果进行操作

图 3

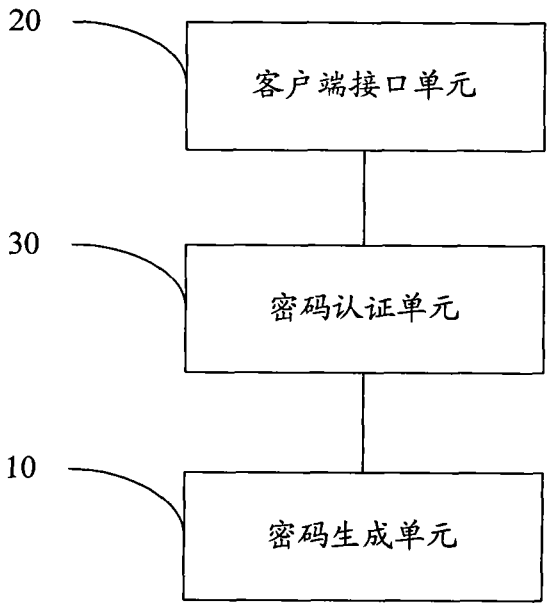

20
客户端接口单元
30
密码认证单元
10
密码生成单元

图 4

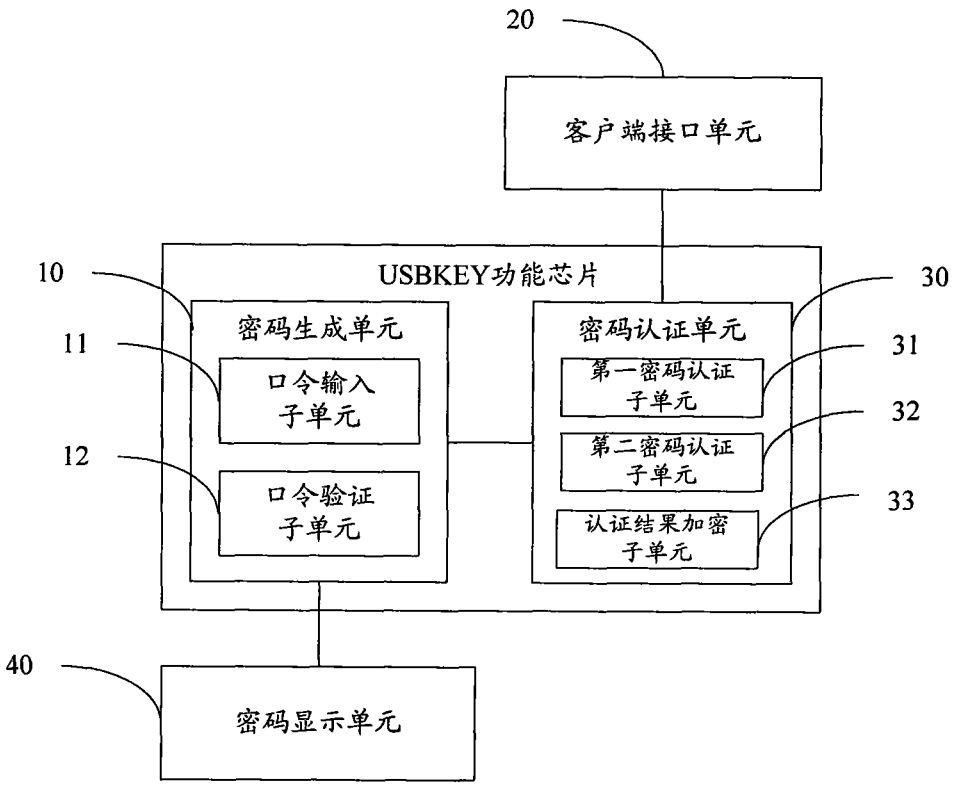

20
客户端接口单元
USBKEY功能芯片
10
密码生成单元
11
口令输入
子单元
12
口令验证
子单元
30
密码认证单元
31
第一密码认证
子单元
32
第二密码认证
子单元
33
认证结果加密
子单元
40
密码显示单元

图 5