[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 9/32 (2006.01)
H04L 9/16 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200610149942.1

[43] 公开日 2008 年 4 月 23 日

[11] 公开号 CN 101166091A

[22] 申请日 2006.10.19
[21] 申请号 200610149942.1
[71] 申请人 阿里巴巴公司
地址 开曼群岛大开曼乔治敦
[72] 发明人 陆兆禧

[74] 专利代理机构 北京集佳知识产权代理有限公司
代理人 逯长明

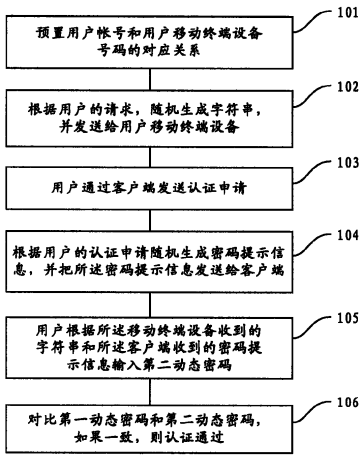
权利要求书 2 页 说明书 10 页 附图 2 页

[54] 发明名称

一种动态密码认证的方法及服务端系统

[57] 摘要

本发明公开了一种动态密码认证的方法，包括：预置用户帐号和用户移动终端设备号码的对应关系；根据用户的请求，随机生成字符串，并发送给用户移动终端设备；根据用户的认证申请随机生成密码提示信息，并把所述密码提示信息发送给客户端，所述密码提示信息规定了所述字符串中特定位的字符组合为本次认证申请的动态密码；用户根据所述移动终端设备收到的字符串和所述客户端收到的密码提示信息输入动态密码；判断用户输入的动态密码的有效性，如果有效，则认证通过。本发明不使用实物密码卡，字符串易于保存，不易丢失；不需要客户进行申请手续，不需要去专门的场所领用和更换，使用方便；攻击者无法使用失密的认证密码通过认证。



1、一种动态密码认证的方法，其特征在于，包括下列步骤：

预置用户帐号和用户移动终端设备号码的对应关系；

根据用户的请求，随机生成字符串，并发送给用户移动终端设备；

根据用户的认证申请随机生成密码提示信息，并把所述密码提示信息发送给客户端，所述密码提示信息规定了所述字符串中特定位的字符组合为本次认证申请的动态密码；

用户根据所述移动终端设备收到的字符串和所述客户端收到的密码提示信息输入动态密码；

判断用户输入的动态密码的有效性，如果有效，则认证通过。

2、根据权利要求 1 所述的方法，其特征在于，在生成密码提示信息之前，还包括：

判断该用户帐号对应的所述随机生成的字符串是否位于有效期内；

如果是，则不再生成新的随机字符串。

3、根据权利要求 1、2 所述的方法，其特征在于，所述字符串是由数字、字母、符号或者三者混合组成的。

4、根据权利要求 1 所述的方法，其特征在于，所述密码提示信息中所规定的特定位是所述字符串中连续的或者是不连续的位。

5、根据权利要求 1 所述的方法，其特征在于，所述认证申请还包括静态密码认证申请，对所述静态密码进行认证，如果认证通过，则继续进行动态密码的认证，否则，认证失败。

6、一种动态密码认证的服务端系统，其特征在于，通过移动通信网络和用户移动终端设备连接，并通过互联网络和用户客户端相连，包括以下部件：

第一存储单元，用于存储用户帐号和用户移动终端号码的对应关系；

字符串生成单元，用于随机生成字符串；

第一动态密码生成单元，根据用户的认证申请随机生成密码提示信息，所述密码提示信息规定了所述字符串中特定位的字符组合为本次认证申请的动态密码；

接口单元，用于将所述字符串发送给所述移动终端设备，并接收用户客户

端发出的认证申请，以及将所述密码提示信息发送给所述用户移动终端设备，接收用户输入的动态密码；

动态密码验证单元，用于判断用户输入的动态密码的有效性，如果有效，则认证通过。

7、根据权利要求 6 所述的系统，其特征在于，所述字符串生成单元还用于判断该用户帐号对应的所述随机生成的字符串是否位于有效期内，如果是，则不再生成新的随机字符串。

8、根据权利要求 6 所述的系统，其特征在于，所述字符串是由数字、字母、符号或者三者混合组成的串。

9、根据权利要求 6 所述的系统，其特征在于，所述密码提示信息中所规定的特定位是所述字符串中连续的或者是不连续的位。

10、根据权利要求 6 所述的系统，其特征在于，还包括：

第二存储单元，用于存储用户帐号以及相应的静态密码；

静态密码验证单元，与第二存储单元相连，用于验证用户输入的静态密码。

一种动态密码认证的方法及服务端系统

技术领域

本发明涉及密码认证领域，特别是涉及一种动态密码认证的方法和服务端系统。

背景技术

在现实生活中，我们个人的身份主要通过各种证件来确认，比如：身份证、户口本等，而计算机的各种系统资源（如：文件、数据和应用系统等）也需要认证机制的保护，从而确保这些资源被适格的人使用。

目前各类计算资源主要通过密码认证方式进行保护，一般使用静态密码认证和动态密码认证两种方式。

静态密码认证方式采用的是“用户名+口令”的认证方式。用户登录时，应用服务器通过静态密码进行身份认证，确认用户是否为合法的授权用户。这种认证的缺点在于：由于用户的帐号是固定的明文，密码是静态的，用户在很长时间内不会更改密码，造成这种密码很容易被窃取；对这种认证方式常用的有效攻击方式有网络数据流窃听、认证信息截取/重放、字典攻击、穷举尝试、窥探、社交工程等；由于这种认证方式存在较多的安全漏洞，对客户的身份进行认证的安全强度已经不能满足现代各类应用系统的要求。

针对静态密码认证的缺点，动态密码认证可以提高认证的安全强度。动态密码也称一次密码，其动态来源于产生密码的运算因子随时间变化。目前网上银行用户在登录网上银行的时候，网上银行会向用户的手机上发送一条短信，告诉用户一个一次性有效的动态密码，用户除了输入客户号、静态密码外，还要输入这个动态密码才能登录网上银行。这样，除了静态密码认证外，用户又多了一重安全保障，而且，由于这个动态密码是每次不同，每个密码只能使用一次，黑客即使窃取了本次的动态密码，也无法再次使用，而且每个动态密码之间毫无规律的，黑客不能猜测出用户的下一个动态密码。这种方式的缺点在于需要依赖于移动通信网络，当移动通信网络出现故障或者手机接收短信故障时，导致用户无法实时接收短信，而动态密码通常会在很短的时间内就失效，影响了用户的登录。

动态密码认证的另一种方式是采用预先发放的密码口令卡进行认证，如，

目前中国工商银行推出网上银行客户使用的电子银行密码口令卡，网上银行客户可申请领取该卡。每张网上银行密码口令卡上都以矩阵形式印有若干字符串。客户通过网上银行进行对外转账、缴费等支付交易时，网上银行系统会随机给出一组口令卡坐标。客户按坐标在卡片上找到正确的口令组合并输入网上银行系统后，才能进行相关交易。密码口令卡的有效使用次数是1000次，超过使用次数时需要申领新卡。这种方式的缺点在于：采用实物密码口令卡，不易保存，容易丢失；使用前，需要客户申请，并去专门场所领取，领用不便；更换时也必须重新申领新的密码口令卡，更换卡不便；有效使用次数较多，造成有效时间长，多数密码在有效期内会被重复使用，容易失密。

总之，现有的密码认证方法都存在一些缺陷，导致密码不能及时接收、不易保存、使用不便和容易失密的问题。

发明内容

本发明所要解决的技术问题是提供一种更方便更安全的动态密码认证的方法和系统，以解决现有技术中密码不能及时接收、不易保存、使用不便和容易失密的问题。

为了解决上述技术问题，本发明公开了一种动态密码认证的方法，包括下列步骤：

预置用户帐号和用户移动终端设备号码的对应关系；

根据用户的请求，随机生成字符串，并发送给用户移动终端设备；

根据用户的认证申请随机生成密码提示信息，并把所述密码提示信息发送给客户端，所述密码提示信息规定了所述字符串中特定位的字符组合为本次认证申请的动态密码；

用户根据所述移动终端设备收到的字符串和所述客户端收到的密码提示信息输入动态密码；

判断用户输入的动态密码的有效性，如果有效，则认证通过。

优选的，在生成密码提示信息之前，所述方法还包括：

判断该用户帐号对应的所述随机生成的字符串是否位于有效期内；

如果是，则不再生成新的随机字符串。

优选的，所述字符串是由数字、字母、符号或者三者混合组成的。

优选的，所述密码提示信息中所规定的特定位是所述字符串中连续的或者是不连续的位。

优选的，所述认证申请还包括静态密码认证申请，对所述静态密码进行认证，如果认证通过，则继续进行动态密码的认证，否则，认证失败。

本发明还提供了一种动态密码认证的服务端系统，通过移动通信网络和用户移动终端设备连接，并通过互联网络和用户客户端相连，包括以下部件：

第一存储单元，用于存储用户帐号和用户移动终端号码的对应关系；

字符串生成单元，用于随机生成字符串；

第一动态密码生成单元，根据用户的认证申请随机生成密码提示信息，所述密码提示信息规定了所述字符串中特定位的字符组合为本次认证申请的动态密码；

接口单元，用于将所述字符串发送给所述移动终端设备，并接收用户客户端发出的认证申请，以及将所述密码提示信息发送给所述用户移动终端设备，接收用户输入的动态密码；

动态密码验证单元，用于判断用户输入的动态密码的有效性，如果有效，则认证通过。

优选的，所述字符串生成单元还用于判断该用户帐号对应的所述随机生成的字符串是否位于有效期内，如果是，则不再生成新的随机字符串。

优选的，所述字符串是由数字、字母、符号或者三者混合组成的串。

优选的，所述密码提示信息中所规定的特定位是所述字符串中连续的或者是不连续的位。

优选的，所述系统还包括：

第二存储单元，用于存储用户帐号以及相应的静态密码；

静态密码验证单元，与第二存储单元相连，用于验证用户输入的静态密码。

与现有技术相比，本发明具有如下优点：

1、使用移动终端设备短信方式传递和保存用于生成动态密码的字符串，不使用实物密码卡，字符串易于保存，不易丢失。

2、由服务器端根据用户请求随机生成字符串，并发送到客户的移动终端设备保存，不需要客户进行申请手续，不需要去专门的场所领用和更换，使用

方便。

3、用于生成动态密码的字符串具有一定的有效期，在有效期内，可以重复使用，客户不需要实时接收短信，移动通信网络故障或延迟对客户身份认证影响小。

4、每次使用时，由服务器端随机确定字符串中的某几位为认证密码，下次使用时，服务器端会再次生成新的认证密码，当某次认证密码失密时，不会造成字符串失密，不会影响下次认证，攻击者无法使用失密的认证密码通过认证。

附图说明

图 1 是本发明的方法流程图；

图 2 是本发明的方法实施例流程图；

图 3 是本发明的系统框图。

具体实施方式

为使本发明的上述目的、特征和优点能够更加明显易懂，下面结合附图和具体实施方式对本发明作进一步详细的说明。

参照图 1，是本发明的方法流程图，具体包括以下步骤：

步骤 101，预置用户帐号和用户移动终端设备号码的对应关系。

在服务器端，预先存储用户的信息，其中包括用户帐号、用户移动终端设备号码等信息，可以要求用户在注册时提供这些信息，或者由其它系统的用户数据导入得到，也可以是由专门的录入员进行信息录入，用户移动终端设备可以是用户的手机、掌上电脑等设备，用户移动设备的编号可以是 SIM 卡（用户身份识别卡）的号码，为了保证用户移动终端设备能顺利接收下面步骤中发给用户的信息，可以在建立用户时，向用户移动终端设备发送验证短信，由用户回填短信中的验证码来确认用户移动终端设备号码正确，这样可以防止信息失密或者短信骚扰。简而言之，就是在服务器端建立了用户帐号和用户移动终端设备号码的对应关系，也可以根据系统的实际需要确认是否需要一对多或者多对一的关系。

步骤 102，根据用户的请求，随机生成字符串，并发送给用户移动终端设备。

所述的字符串将在后续步骤中用于产生用户的认证密码，关于如何产生的问题将在后文中介绍。所述字符串采用随机生成的方式产生，字符串的位数可以根据需要任意确定，理论上可以是1到无穷大，字符串的位数越大，可以生成的动态密码的位数就可以越大，密码认证的安全性就可以越高，考虑传送字符串和用户查阅字符串方便性，可以将字符串限制在一个合理的长度，字符串的生成可以采用程序设计语言中的随机函数生成，也可以自行编写函数实现。生成字符串后，把字符串绑定到用户帐号上，可以用户帐号和字符串对应关系保存在服务器端，绑定后，把字符串发送给用户移动终端设备，用于用户产生动态密码之用。

服务器端可以使用短信方式把所述字符串发送给用户移动终端设备。移动终端设备也可以采用其他方式获取字符串，例如，可以由服务器端发送一个网址给移动终端设备，移动终端设备按照网址上网找到需要的字符串。

用户的请求信息可以是注册申请、重要操作申请或者是要求更新字符串的申请等，由这些申请来触发服务器端生成字符串。

优选的，所述随机生成的字符串具有一定的有效期，由服务器端判断所述字符串是否超期，如果超期，重新生成字符串并发送给用户移动终端设备，若否，不再生成新的字符串，继续使用原字符串。也可以判断是否在以当前时间倒推一个有效期的时间内是否给用户帐号发送过字符串的，如果发送过，则认为所发送的字符串仍然有效，如果没有发送过，则认为所述字符串已经失效，需要重新生成。设置有效期的目的是为了定期更新字符串，从而进一步提高动态密码的安全性，防止字符串失密。这里也可以设定字符串的使用次数代替有效期，当字符串使用超过一定次数，例如50次，则认为字符串失效，需要重新生成字符串。有效期设置的过长，可能会增大失密的危险，设置的过短，字符串的更新过于频繁，用户需要经常更新保存的字符串，使用上不方便，在实际使用中，可以根据需要确定一个合适的有效期来兼顾安全性和使用的方便性。

优选的，所述字符串既可以是由数字组成，也可以是由字母或者符号组成，还可以是由三者混合组成，这样可以增大由字符串生成的密码空间，进一步增加安全性。所述字符串的形式可以是一维的，以便于用户移动终端设备接收、

显示和查阅。

步骤 103，用户通过客户端发送认证申请。

当用户需要进行身份认证时，可以是用户登录时或者进行某项安全性要求较高的操作（如网上银行的支付操作）时，用户可以通过客户端向服务器端发出认证申请，认证申请中可以包含用户的帐号等信息。

步骤 104，根据用户的认证申请随机生成密码提示信息，并把所述密码提示信息发送给客户端，所述密码提示信息规定了所述字符串中特定位的字符组合为本次认证申请的第一动态密码。

服务器端为每次用户的认证请求随机生成不同的密码提示信息。可以采用计算机中的随机算法函数或者自己编写的函数实现随机生成密码提示信息，这样每次生成的密码提示信息都不相同，密码提示信息只能在本次认证请求中使用，对于新的认证请求，将生成新的密码提示信息。为进一步增加安全性，还可以在生成的密码提示信息上附加时间戳标记，使其在一定时间后失效。

优选的，所述密码提示信息中所规定的特定位可以是所述字符串中连续的或者是不连续的位。

例如，服务器端产生了“322h4b432y”的字符串，已经和用户帐号绑定，并发送给了用户，服务器端通过随机算法确定了“64814”的随机数串，产生如下的密码提示信息：“顺次提取字符串第 6、4、8、1、4 位作为认证密码”，则从“322h4b432y”中顺次提取第 6、4、8、1、4 位得到的第一动态密码是“bh33h”，保存在服务端，并把密码提示信息发送给用户。发送的方式可以是通过 http 方式，显示在返回给客户端的认证页面上。

步骤 105，用户根据所述移动终端设备收到的字符串和所述客户端收到的密码提示信息输入第二动态密码。

用户接收到服务器端发送的密码提示信息后，操作移动终端设备显示出预先接收到的字符串，根据密码提示信息从字符串中提取出第二动态密码，作为认证密码发送给服务器端。发送的方式可以是由用户在客户端的认证页面上输入，并提交给服务器端。

例如，用户预先收到的字符串是“322h4b432y”，得到的密码提示信息是“顺次提取字符串第 6、4、8、1、4 位作为认证密码”，则用户取得的第二动

态秘密是“bh33h”，用户将第二动态密码输入到客户端的认证页面上，提交给服务器端。

步骤106，对比第一动态密码和第二动态密码，如果一致，则认证通过。

服务器端接收到用户提交的第二动态密码，取出在步骤104中生成的第一动态密码，进行比对，如果密码一致，则用户认证通过，允许用户进行登录或者其他操作，如果密码不一致，认证失败，发送提示信息给用户，提示用户认证失败，不允许用户登录或者其他操作。

优选的，上述步骤还包括，用户通过客户端向服务器端发送的认证申请中还包括预先设定的静态密码，客户端把静态密码和用户信息发送给服务器端，经过和预先保存的用户的静态密码比对后，确定用户静态密码是否认证通过，如果认证通过，则继续进行动态密码的认证，如果认证未通过，提示用户认证失败。也可以先进行动态密码验证，如果验证通过，再进行静态密码验证。也可以采用动态密码和静态密码同时验证的方式，当两者验证都通过时认为用户认证通过，有一项未通过时，认证失败。对于非法获得用户字符串的用户，在缺少用户帐号、当前动态密码和静态密码其中之一时，无法登录系统，同时，还可以结合多次错误输入或者增加校验码等技术防止攻击者的穷举式非法扫描。

在上述方法中，所述用户移动终端设备可以是手机或掌上电脑等设备。

下面以用户在电子商务网站进行支付操作时的身份认证为例进一步进行介绍。

参照图2，是本发明的方法实施例流程图，具体包括以下步骤：

步骤201，用户登录电子商务网站。

用户可以是预先注册过的电子商务网站用户，并且通过了电子商务网站的资格认证（如验证了个人信息的真实性、拥有合法的交易资金帐号等），并且验证过用户手机号码的正确性。

步骤202，如果用户帐号未绑定在有效期内的用于生成动态密码的字符串，电子商务网站向用户手机发送短信，该短信内容为一串数字或一串字符组成的字符串。

对于未绑定在有效期内的字符串的用户帐号，电子商务网站采用随机算法

生成一个字符串，该字符串可以由数字、字母和符号组成。并根据预先保存的用户移动终端设备号码通过移动通信网络发送短信，短信中包含所述生成的字符串。

步骤203，用户提交支付请求，电子商务网站生成密码提示信息和第一动态密码，并在返回给用户的支付操作页面上显示密码提示信息和密码输入框。

步骤204，用户按照密码提示信息从手机接收到的字符串中取得第二动态密码，输入到电子商务网站的支付操作页面上并提交。

步骤205，电子商务网站对比第一动态密码和第二动态密码，如果一致，允许用户进行支付操作。

电子商务网站为用户手机接收到的字符串设定一定的有效期，该有效期时间可以较长，而且只要在有效期内，该字符串并不是一次失效，只要通过电子商务网站变更密码提示信息，更换输入字符串的位数就可实现该字符串的反复使用。

参照图3，是本发明的服务端系统框图，具体包括：

移动终端设备301，用于接收和保存服务端系统发送的字符串；

客户端302，用于发送用户的认证申请，接收服务端系统发送的密码提示信息，以及向服务端系统发送用户输入的第二动态密码；

服务端系统303，通过移动通信网络和移动终端设备301连接，并通过互联网络和客户端302相连，包括以下部件：

字符串生成单元3031，用于生成随机的字符串；

第一存储单元3032，用于存储用户帐号和用户移动终端号码的对应关系；

第一动态密码生成单元 3033，用于根据用户的认证申请随机生成密码提示信息，并根据密码提示信息生成第一动态，所述密码提示信息规定了所述字符串中特定位的字符组合为本次认证申请的动态密码；

接口单元3034，用于将所述字符串发送给所述移动终端设备301，并接收客户端302发出的认证申请，以及将所述密码提示信息发送给所述移动终端设备301，接收客户端302发送的第二动态密码；

动态密码验证单元3035，用于比对第一密码和第二动态密码，如果一致，则认证通过。

字符串生成单元 3031 根据用户请求为用户帐号随机生成一个字符串，字符串的位数可以根据需要任意确定，理论上可以是 1 到无穷大，考虑传送字符串和用户查阅字符串方便性，可以将字符串限制在一个合理的长度，字符串的生成可以采用程序设计语言中的随机函数生成，也可以自行编写函数实现。生成字符串后，把字符串绑定到用户帐号上，绑定后，把字符串发送给用户移动终端设备 301。当用户需要进行身份认证时，可以是当用户进行某项安全性要求较高的操作（如网上银行的支付操作）时，用户可以通过客户端 302 向服务端系统 303 的接口单元 3034 发出认证申请，认证申请中可以包含用户帐号等信息。接口单元 3034 收到用户提交的认证申请后，由第一动态密码生成单元 3033 找到由字符串生成单元 3031 生成的和用户帐号绑定的字符串，第一动态密码生成单元 3033 根据随机算法生成密码提示信息，密码提示信息描述了从字符串中提取若干位作为第一动态密码，并根据密码提示信息生成第一动态密码。接口单元 3034 把密码提示信息发送给客户端 302。用户接收到密码提示信息后，操作移动终端设备 301 显示出接收到的字符串，根据密码提示信息从字符串中提取出第二动态密码，作为认证密码发送给服务端系统 303 的接口单元 3034。发送的方式可以是由用户在客户端 303 上显示的认证页面上输入，并提交。接口单元 3034 接收到用户提交的第二动态密码，发送给动态密码验证单元 3035，和保存的第一动态密码进行比对，如果密码一致，则用户认证通过，允许用户进行操作，如果密码不一致，认证失败，发送提示信息给用户，提示用户认证失败，不允许用户进行操作或者引导用户重新进行认证。

优选的，所述随机生成的字符串具有一定的有效期，由字符串生成单元 3031 判断所述字符串是否超期，如果超期，重新生成字符串并发送给用户移动终端设备，若否，不再生成新的字符串，继续使用原字符串。判断是否超期也可以采用下面的方法：判断所述字符串是否在有效期内、判断是否在以当前时间倒推一个有效期的时间内是否给用户帐号发送过字符串的或者所述的字符串使用次数是否达到一定的数值。

优选的，所述字符串既可以是由数字组成，也可以是由字母或者符号组成，还可以是由三者混合组成。

优选的，第一动态密码生成单元 3033 为每次用户的认证请求随机生成不

同的密码提示信息。可以采用计算机中的随机算法函数或者自己编写的函数实现随机生成密码提示信息，这样每次生成的密码提示信息都不相同，密码提示信息只能在本次认证请求中使用，对于另一次的认证请求，将生成新的密码提示信息。为进一步增加安全性，还可以在生成的密码提示信息上附加时间戳标记，使其在一定时间后失效。

优选的，所述密码提示信息中所规定的特定位可以是所述字符串中连续的或者是不连续的位。

优选的，服务端系统 303 还可以包括:

第二存储单元 3036，用于存储用户帐号以及相应的静态密码;

静态密码验证单元 3037，与第二存储单元相连，用于验证用户输入的静态密码。

用户通过客户端 302 向服务端系统 303 的接口单元 3034 发送的认证申请中还包括预先设定的静态密码，客户端 302 把静态密码和用户信息发送给服务端系统 303 的接口单元 3034，经过和预先保存在第二存储单元 3036 的用户的静态密码比对后，静态密码验证单元 3037 确定用户静态密码是否认证通过，如果认证通过，则继续进行动态密码的认证，如果认证未通过，提示用户认证失败。也可以先进行动态密码验证，如果验证通过，再进行静态密码验证。也可以采用动态密码和静态密码同时验证的方式，当两者验证都通过时认为用户认证通过，有一项未通过时，认证失败。

本发明的一种动态密码认证的方法和系统可用于游戏、金融、证券、商业、政府、学术、企业计算机系统登陆以及企业虚拟专用网。

以上对本发明所提供的一种密码认证的方法和系统，进行了详细介绍，本文中应用了具体个例对本发明的原理及实施方式进行了阐述，以上实施例的说明只是用于帮助理解本发明的方法及其核心思想; 同时，对于本领域的一般技术人员，依据本发明的思想，在具体实施方式及应用范围上均会有改变之处，综上所述，本说明书内容不应理解为对本发明的限制。

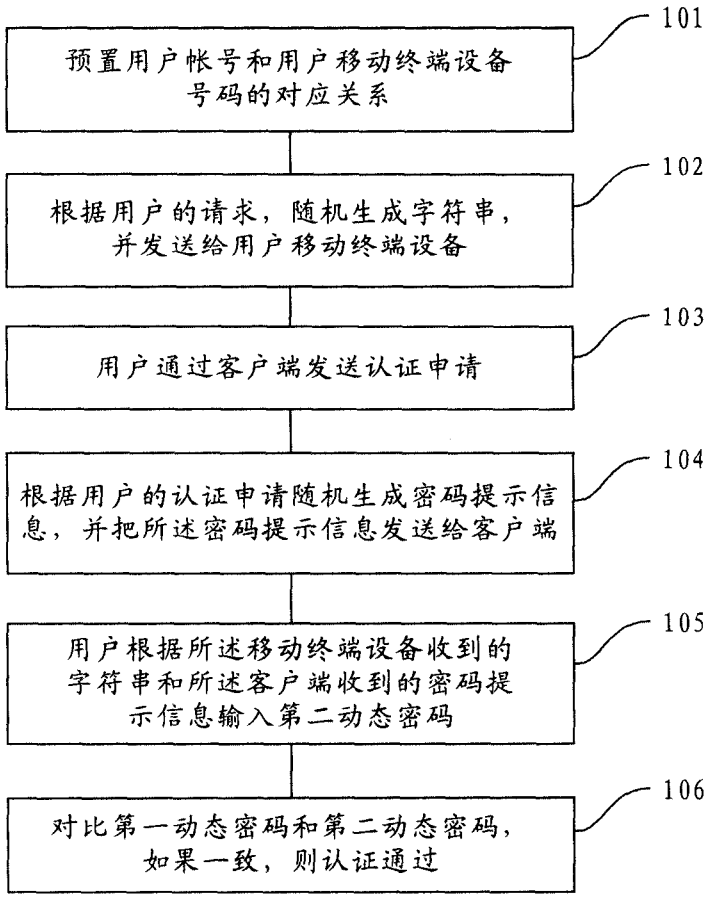

101
预置用户帐号和用户移动终端设备号码的对应关系
102
根据用户的请求，随机生成字符串，并发送给用户移动终端设备
103
用户通过客户端发送认证申请
104
根据用户的认证申请随机生成密码提示信息，并把所述密码提示信息发送给客户端
105
用户根据所述移动终端设备收到的字符串和所述客户端收到的密码提示信息输入第二动态密码
106
对比第一动态密码和第二动态密码，如果一致，则认证通过

图 1

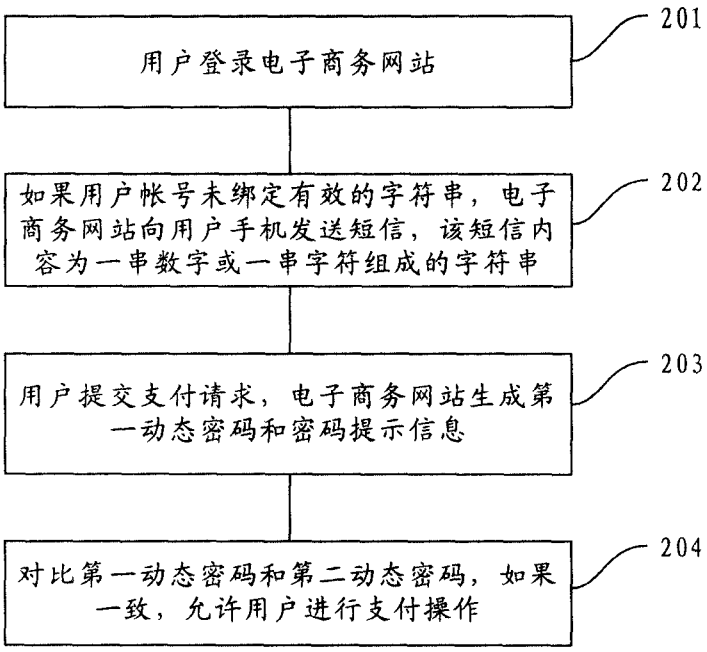

用户登录电子商务网站
201
如果用户帐号未绑定有效的字符串，电子商务网站向用户手机发送短信，该短信内容为一串数字或一串字符组成的字符串
202
用户提交支付请求，电子商务网站生成第一动态密码和密码提示信息
203
对比第一动态密码和第二动态密码，如果一致，允许用户进行支付操作
204

图 2

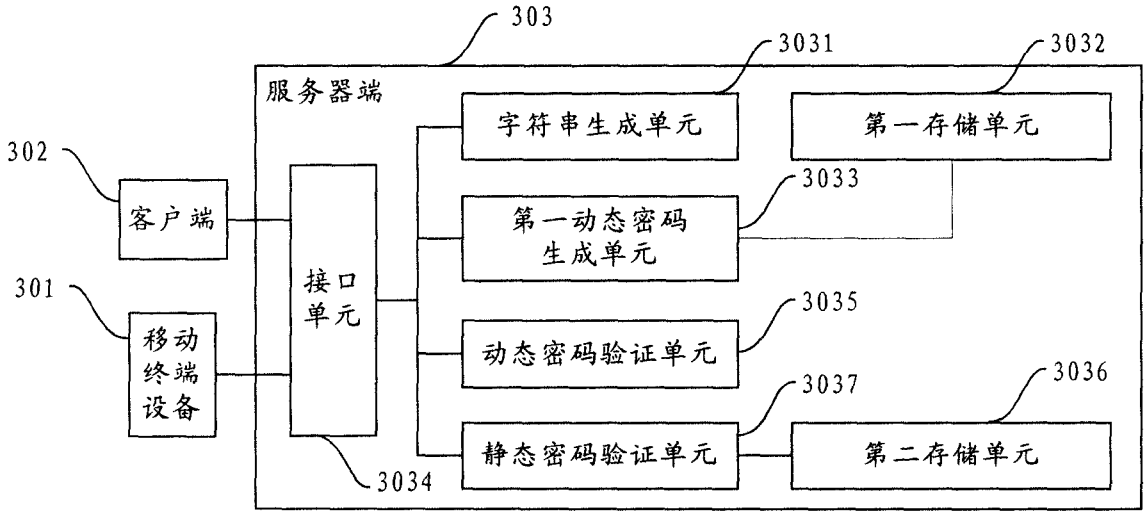

303
服务器端
3031
字符串生成单元
3032
第一存储单元
302
客户端
3033
第一动态密码生成单元
301
移动终端设备
接口单元
3035
动态密码验证单元
3037
3036
静态密码验证单元
第二存储单元
3034

图 3