[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
H04L 9/16

[12] 发明专利申请公开说明书

[21] 申请号 200510069255.4

[43] 公开日 2005 年 11 月 9 日

[11] 公开号 CN 1694396A

[22] 申请日 2005.5.12
[21] 申请号 200510069255.4
[71] 申请人 北京易诚世纪科技有限公司
地址 100085 北京市海淀区上地信息路 28 号信息大厦 A 座 11 层
[72] 发明人 张 岩 曾 硕

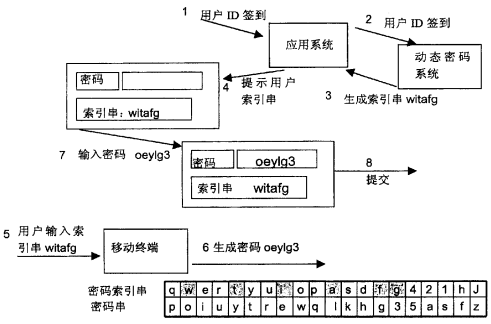
[74] 专利代理机构 北京三友知识产权代理有限公司
代理人 任默闻

权利要求书 3 页 说明书 10 页 附图 3 页

[54] 发明名称 一种动态密码方法及系统

[57] 摘要

本发明涉及加密领域，其特别涉及一种动态密码方法及系统。 用户端拥有至少一个索引符号和至少一个密码符号，建立所述索引符号和密码符号之间的对应关系；由运营端生成动态密码，并根据所述索引符号和密码符号之间的对应关系，向用户端提供当前动态密码所对应的索引符号；用户端即得到索引符号所对应的动态密码。 本发明的有益效果在于，省去了现有动态密码系统中用户端专用的密码计算器，降低了成本并且保证了相当的安全性，密码系统算法多样性强，更加符合用的需求。



ISSN1008-4274

1. 一种动态密码方法，其特征在于，用户端拥有至少一个索引符号和至少一个密码符号，建立所述索引符号和密码符号之间的对应关系；由运营端生成动态密码，并根据所述索引符号和密码符号之间的对应关系，向用户端提供当前动态密码所对应的索引符号；用户端即得到索引符号所对应的动态密码。

2. 根据权利要求1所述的一种动态密码方法，其特征在于在运营端向用户端提供动态密码所对应的索引符号前还包括一用户端与运营端索引符号和密码符号之间对应关系的同步步骤，在该步骤中由用户设置运营端提供给用户的与当前动态密码所对应索引符号的变化规则。

3. 根据权利要求1、2任一项所述的一种动态密码方法，其特征在于所述索引符号和密码符号之间的对应关系由用户制定，并通知运营端。

4. 根据权利要求1、2任一项所述的一种动态密码方法，其特征在于所述索引符号和密码符号之间的对应关系由运营端制定。

5. 根据权利要求1所述的一种动态密码方法，其特征在于所述对应关系为由至少一个索引符号对应一个密码符号。

6. 根据权利要求1所述的一种动态密码方法，其特征在于所述的索引符号是指数字、字母、标点、标示符号其中一种或是多种的组合。

7. 根据权利要求1所述的一种动态密码方法，其特征在于所述的密码符号是指数字、字母、标点、标示符号其中一种或是多种的组合。

8. 根据权利要求1所述的一种动态密码方法，其特征在于所述索引符号和密码符号及其对应关系存储于用户端的加密卡或者移动通信终端中。

9. 根据权利要求8所述的一种动态密码方法，其特征在于所述加密卡为纸制品，塑料制品，金属制品。

10. 根据权利要求8所述的一种动态密码方法，其特征在于所述移动通信终端通过多媒体信息方式或者动态密码模块方式存储、处理所述索引符号和

所述的密码符号。

11. 根据权利要求10所述的一种动态密码方法，其特征在于所述利用移动通信终端的动态密码方法包括：步骤1，用户在应用系统上输入用户序列号；步骤2，应用系统与后台的动态密码装置通信；步骤3，按照索引符号和密码符号的对应关系，动态生成密码符号串和相对应的索引符号串，并把索引符号串传送给应用系统；步骤4，在应用系统的界面上显示索引符号串，并提示用户输入相应的密码符号串；步骤5，用户根据应用系统界面显示的索引符号串启动手机或是其他移动终端上的动态密码模块；步骤6，该动态密码模块中储存有索引符号和密码符号的对应关系，根据用户输入的索引符号串找到对应的密码符号串，并显示在移动终端的屏幕上；步骤7，用户根据移动终端显示的密码符号串在应用系统显示界面上输入密码符号串；步骤8，应用系统得到该密码符号串后向动态密码装置传送该密码符号串，由动态密码装置验证该密码符号串是否与生成的动态密码符号串相一致。

12. 根据权利要求1或11所述的一种动态密码方法，其特征在于如果用户输入错误的动态密码则记录该次登录，并且判断错误输入的次数，累计到一定次数则拒绝用户输入密码。

13. 一种动态密码系统，其特征在于包括：

动态密码装置，用于生成动态密码，管理与维护动态密码；

后台应用系统，与所述动态密码装置相连接，完成用户的身份确认；

用户输入终端，与所述动态密码装置相连接，用于显示及输入用户信息及密码；

用户端动态密码单元，所述动态密码单元上具有至少一个索引符号，至少由一个索引符号对应一个密码符号，所述动态密码装置提供当前动态密码所对应的至少一个索引符号显示在用户输入终端，并且用户在该用户输入终端输入该至少一个索引符号所对应的密码符号，输入的密码符号正确则通过用户的身份确认，允许用户进入系统完成相关操作。

14. 根据权利要求13所述的一种动态密码系统，其特征在于所述用户端动态密码单元包括密码卡或者移动通信终端或者移动终端。

15. 根据权利要求14所述的一种动态密码系统，其特征在于所述密码卡为纸制品，塑料制品，金属制品。

16. 根据权利要求14所述的一种动态密码系统，其特征在于所述移动通信终端或者移动终端包括：移动电话，PDA，计算机，计算器。

一种动态密码方法及系统

技术领域

本发明涉及加密领域，其特别涉及一种动态密码方法及系统。

背景技术

目前，各服务机构提供的身份验证方法多是为客户提供一个静态密码。用户在接受服务机构提供的电子自动交易服务时，服务机构与用户之间通过这个静态密码进行身份验证，完成交易或商品的发送。但是，这种身份的验证方法非常不安全，因为这种静态密码很容易被他人破译，而且破译这种静态密码的方法很多也很容易，如：采用计算机技术截获数据、人工盗窃、内外勾结骗盗等手段获取用户的静态密码，冒领客户存款，此类事件经常见诸报端。这给人们使用电子手段从事社会经济生活带来了很大的风险，同时也给正在兴起的电子自动交易（如电子商务、电子支付等）的发展带来了机器不利的影响，阻碍了这些行业向更深更远的方向发展。

数字证书加密技术可以对网络上传输的信息进行加密和解密、数字签名和签名验证，确保网上传递信息的机密性、完整性，以及交易实体身份的真实性等，签名信息的不可否认性，从而保障网络应用的安全性。数字证书最大程度上增强了通讯过程中的安全性，但需要存储介质(USB或者其他介质的存储卡)才能保存使用，“基于U盘的证书系统”,该设备认证系统的基本思路是:在U盘中存储证书信息，做到证书随身走，但是这种设备增加了整个认证系统的成本，如果证书丢失，后果仍然像上述一样严重。并且采用行业中流行的证书要缴纳高昂的使用费，安装起来也不方便，必须每个使用者都在计算机中进行软件的安装，对于一个计算机水平不高的普通使用者来说困难是可想而知的。

目前出现了动态密码机制，动态密码(Dynamic Password)也称一次性密码(One-time Password)。动态密码是变动的密码，其变动来源于产生密码的运算因子是变化的。动态密码的产生因子一般都采用双运算因子(Two Factor)：其一，为用户的私有密码。它代表用户身份的识别码，是固定不变的。其二，为变动因子。正是变动因子的不断变化，才产生了不断变动的动态密码。采用不同的变动因子，形成了不同的动态密码认证技术：基于时间同步（Time Synchronous）认证技术、基于事件同步（Event Synchronous）认证技术和挑战/应答方式的非同步（Challenge/Response Asynchronous）认证技术。

基于时间同步认证技术是把流逝的时间作为变动因子，一般以 60 秒作为变化单位。所谓“同步”，是指用户密码卡和认证服务器所产生的密码在时间上必须同步。这里的时间同步方法不是用“时统”技术，而是用“滑动窗口”技术。图为客户终端访问系统时，基于时间同步的认证过程。用户端的终端和服务器端的时钟同步，在用户使用密码时要利用用户终端生成动态的密码与服务器的动态密码相匹配，否则不能通过服务器的密码认证，这种系统同样需要用户终端的高额成本。

中国发明专利 03106069.2 中所揭示的一种动态数据密码输入方法及装置，其方法为：提供给操作者输入选择的数据跳变单元自动处于动态变化状态，以使操作者不同时刻确认的内容随数据跳变单元所表示的含义而定；直到操作者输入全部密码，系统读入并保存操作者输入的全部数据，并对读入并保存的数据进行唯一性判断，当系统读入并保存的数据是唯一的时，该唯一数据即为操作者输入密码。但是该方法没有对密码等信息进行真正的动态运算，只是在输入界面上作了跳变的处理，安全性不高。

中国发明专利 00109820.9 揭示了一种采用动态密码的认证付款的方法和相应的电子装置，由动态密码认证装置经转发中心向用户和直接向商户或银行发出一随机产生的同一天码，用户向商户或银行输入上述天码和商户或银行事先给予用户的心码共同组成的动态密码，供商户或银行进行核对。但是

这种方法需要第三方参与，并且需要经过邮件或者手机短信息等方式通知用户今天的密码，加密的工作全由服务端完成用户只是简单的接收密码，这样造成了进一步泄密的可能，并且使用起来并不方便，用户在每次交易的时候都需要从动态密码认证装置经转发获得密码，从用户来说密码的获得是被动的。

发明内容

本发明正是鉴于解决上述问题而提出的，因此本发明的目的在于提供一种动态密码的身份认证方法及系统。利用服务器端密码的动态变化提示用户密码变化的方式，由用户输入相应密码，以保证用户密码的动态变化，提高系统如用户账户的安全性。

一种动态密码方法，用户端拥有至少一个索引符号和至少一个密码符号，建立所述索引符号和密码符号之间的对应关系；由运营端生成动态密码，并根据所述索引符号和密码符号之间的对应关系，向用户端提供当前动态密码所对应的索引符号；用户端即得到索引符号所对应的动态密码。

在运营端向用户端提供动态密码所对应的索引符号前还包括一用户端与运营端索引符号和密码符号之间对应关系的同步步骤，在该步骤中由用户设置运营端提供给用户的与当前动态密码所对应索引符号的变化规则。

所述索引符号和密码符号之间的对应关系由用户制定，并通知运营端。

所述索引符号和密码符号之间的对应关系由运营端制定。

所述对应关系为由至少一个索引符号对应一个密码符号。

所述的索引符号是指数字、字母、标点、标示符号其中一种或是多种的组合。

所述的密码符号是指数字、字母、标点、标示符号其中一种或是多种的组合。

所述索引符号和密码符号及其对应关系存储于用户端的加密卡或者移动通信终端中。

所述加密卡为纸制品，塑料制品，金属制品。

所述移动通信终端通过多媒体信息方式或者动态密码模块方式存储、处理所述索引符号和所述的密码符号。

所述利用移动通信终端的动态密码方法包括：步骤1，用户在应用系统上输入用户序列号；步骤2，应用系统与后台的动态密码装置通信；步骤3，按照索引符号和密码符号的对应关系，动态生成密码符号串和相对应的索引符号串，并把索引符号串传送给应用系统；步骤4，在应用系统的界面上显示索引符号串，并提示用户输入相应的密码符号串；步骤5，用户根据应用系统界面显示的索引符号串启动手机或是其他移动终端上的动态密码模块；步骤6，该动态密码模块中储存有索引符号和密码符号的对应关系，根据用户输入的索引符号串找到对应的密码符号串，并显示在移动终端的屏幕上；步骤7，用户根据移动终端显示的密码符号串在应用系统显示界面上输入密码符号串；步骤8，应用系统得到该密码符号串后向动态密码装置传送该密码符号串，由动态密码装置验证该密码符号串是否与生成的动态密码符号串相一致。

如果用户输入错误的动态密码则记录该次登录，并且判断错误输入的次数，累计到一定次数则拒绝用户输入密码。

一种动态密码系统，包括：

动态密码装置，用于生成动态密码，管理与维护动态密码；

后台应用系统，与所述动态密码装置相连接，完成用户的身份确认；

用户输入终端，与所述动态密码装置相连接，用于显示及输入用户信息及密码；

用户端动态密码单元，所述动态密码单元上具有至少一个索引符号，至少由一个索引符号对应一个密码符号，所述动态密码装置提供当前动态密码所对应的至少一个索引符号显示在用户输入终端，并且用户在该用户输入终端输入该至少一个索引符号所对应的密码符号，输入的密码符号正确则通过

用户的身份确认，允许用户进入系统完成相关操作。

所述用户端动态密码单元包括密码卡或者移动通信终端。

所述密码卡为纸制品，塑料制品，金属制品。

所述移动通信终端包括：移动电话，PDA，计算机，计算器。

本发明的有益效果在于，随机生成的密码序列使得用户每次登录密码不确定，即使采用网络监听、暴力破解、关联猜测也无法破解；密码的强度很高；由于密码的变化性、不确定性也省去了用户修改密码的日常操作，达到了经常修改密码的目的；通过其他保护措施保证即使存储密码串的介质（如密码卡片）丢失也可以保证用户密码的安全性，省去了现有动态密码系统中用户端专用的密码计算器，降低了成本，具有安全性较高、投资成本低、适用范围广、与应用集成相对容易等优点。

附图说明

图1为本发明用户端动态密码卡示意图；

图2为本发明另一种用户端动态密码卡示意图；

图3为网上银行应用本发明嵌入式动态密码系统示意图；

图4为企业内部应用本发明独立动态密码系统示意图。

图5为本发明使用移动终端作为动态密码串的存储介质示意图。

具体实施方式

下面，结合附图对于本发明进行如下详细说明。

如图 1 所示为本发明用户端动态密码卡示意图。为了降低用户端动态密码卡的成本，可以采用纸制品或者是塑料制品作为用户账号，索引符号和密码符号的载体，在索引符号和密码符号的表面涂覆保护层，用以防止强光探照等方法得知索引符号和密码符号。其中索引符号和密码符号可为任意符号，包括：字母，数字，标点符号，其他字符。在本例中索引符号为单一的数字，密码符号为大写字母，小写字母或者数字的混合类型，在这里每一组

索引符号对应一个密码符号，例如第一组索引符号“1”对应密码符号“e”，第二组索引符号“2”对应密码符号“u”。

如图 2 所示为本发明另一种用户端动态密码卡示意图。图中每组索引符号采用 2 个符号组成，一个符号代表行，一个符号代表列，构成一个矩阵，每一行和每一列对应不同的密码符号，例如第 1 组索引符号“11”所对应的密码符号为“a”，另一组索引符号“12”对应的密码符号为“b”，索引符号“45”代表密码符号“t”。

如图 5 所示为本发明的实用移动终端的动态密码卡示意图。用户的索引符号和密码符号均由用户自行设定，以网络的方式传送到服务器端，同时设定到用户的移动终端上。在系统需要进行身份确认要求用户输入密码时，会提示用户密码索引串，用户将索引串输入到移动终端的动态密码模块中，动态密码模块将根据输入的索引符号串和事先设定的密码符号串生成动态密码。步骤 1，当用户在密码的输入终端（应用系统）上输入用户序列号；步骤 2，应用系统与后台的动态密码装置通信；步骤 3，按照事先用户传送给动态密码装置的索引和密码对应表，动态生成密码符号串和相对应的索引符号串，并把索引符号串传送给应用系统；步骤 4，在应用系统的界面上显示索引符号串，并提示用户输入相应的密码符号串；步骤 5，用户根据应用系统界面显示的索引符号串启动手机或是其他移动终端上的动态密码模块；步骤 6，该动态密码模块储存于手机或是其他移动终端的存储器中，并且在该动态密码模块中存储有用户设置的索引和密码对应列表，根据用户输入的索引符号串找到对应的密码符号串，并显示在移动终端的屏幕上；步骤 7，用户根据移动终端显示的密码符号串在应用系统显示界面上输入密码符号串；步骤 8，应用系统得到该密码符号串后向动态密码装置传送该密码符号串，由动态密码装置验证该密码符号串是否与生成的动态密码符号串相一致。

作为另一个实施例上面所述的移动终端或者手机也可以接收动态密码装置发送的图片形式或者是列表形式的索引符号串和密码符号串的对应关

系表，这种图片或者列表可以通过多媒体短信息方式法送，如图 1 所示的对应关系表，用户根据该对应关系表进行每次密码的输入。

图3所示为应用本发明的网上银行系统示意图。网上银行系统具有以下的特征：用户数量大——尤其是大众版用户，安全要求高——尽管没有充裕的资金或者需求来购买证书，大众版的用户仍然希望提供对其网上银行账户的更多保护，性能要求高——网上银行的运行要求7x24小时，在用户期望的返回时间内，高峰期的业务处理的能力要求非常高。

鉴于以上的网上银行的特征，采用嵌入式动态密码系统，以最小的成本来提高用户的安全级别降低银行经营风险保证网上银行系统的运行性能。

首先用户在拿到用户端动态密码卡后需要上网或是打电话方式将动态密码卡激活，也就是使银行端的动态密码装置开始运算，并且在这过程中也可以设定用户自己的索引符号序列和所对应的密码符号序列，这些用户信息均存储在动态密码装置中，该动态密码装置根据每个用户端的存储信息（包括用户指定的索引符号序列和密码符号序列，或者用户使用密码卡自带的索引符号序列和密码符号序列）在生成动态密码，当用户向个人网上银行、对公网上银行、银企互联等发起连接或交易请求时，网上银行核心交易平台启动动态密码装置获得当前时刻的动态密码并存入缓存，生成的动态密码符号都是用户端密码卡的密码符号中的符号，根据动态密码装置由用户启动同步时留下的信息结合用户端动态密码卡的索引符号和密码符号，将本次生成的动态密码转换成相应的索引符号，提示用户输入相应某几个索引符号所对应的密码符号，结合图1如果动态密码装置产生的动态密码为：eu8u，则应提示用户输入该用户端动态密码卡上第1个、第2个、第4个、第5个索引符号所对应的密码符号，用户参照动态密码卡即可以输入“eu8u”，当动态密码装置接收到用户输入的密码后与缓存中的动态密码相比较，如果两者相同则证明用户身份，可以在网上银行进行交易，如果两者不同则由动态密码装置再次生成一动态密码，要求用户进行第2次输入，如果用户的密码输入尝试超过一定

次数，比如3次，则记录下该用户最后输入尝试的时间，并拒绝服务一段时间，以起到防止非动态密码卡所有者进行输入尝试的目的。

如上所述在提示用户的密码索引符号时可以通过运营端将索引符号通过变形生成图形的方式提示用户，增强保密性防止网络截获。

对于大众版用户，登录环节：

在每次登录时，根据系统提示的动态密码位置输入相应的密码串，其手续没有太多的增加；

客户服务环节：

在网上银行的相应客户服务页面中提供密码的一些管理功能，如：密码偏移设置、密码作废规则管理等；

网上银行核心交易平台：

加入动态密码卡片的相应控制步骤。如：动态密码校对、动态密码偏移设置、动态密码作废规则设置。

个人网上银行系统：

增加客户服务功能，如：密码偏移设置、密码作废规则管理等；

登录流程中，将原来的密码比对部分用动态密码校对的控制步骤进行替换；

内部管理系统：

用户注册流程，对于非证书的用户注册流程，增加发放动态密码卡的步骤；

增加动态密码卡的挂失、规则维护等功能模块。

进一步，为了加强动态密码的保密性还可以采用偏移技术。偏移技术就是在用户根据动态密码卡与动态密码装置进行同步时选择偏移量，当客户发出密码校验请求时，系统提示的索引符号须按照客户预先定义的偏移量进行重组，此重组的索引符号序列所对应的密码符号才是此次客户应当输入的登录密码（如若超出则循环）。例如：客户A的密码串如图1所示；设定的统一

向右偏移量为1；系统提示索引符号序列为：20、1、3、4，输入者如果不知道偏移的方向或者偏移量就是直接输入：rej8，用户此次登录的真实索引符号序列应为：1(20+1，进行循环)、2(1+1)、4(3+1)、5(4+1)。由此可知该客户此次登陆的密码应该为：eu8u。同时也可以设定的统一向左偏移量为1；系统提示索引符号序列为：2、3、5、6，输入者如果不知道偏移的方向或者偏移量就会直接输入：uju6,但是用户此次登录的真实索引符号序列应为：1(2-1)、2(3-1)、4(5-11)、5(6-1)。由此可知该客户此次登陆的密码应该为：eu8u。

设定不同的偏移量：当客户发出密码校验请求时，系统提示的索引符号须按位按照客户预先定义的偏移量进行重组，此重组的索引符号序列才是此次客户应当输入的登陆密码（如若超出则循环）。例如：客户A的密码符号矩阵如图2所示；设定统一为以行为基础向右循环偏移量1、2、3、4；生成的密码为：abty，动态密码装置则提示用户输入索引符号序列为：15（第1行第5列）、15（第1行第5列）、42（第4行第2列）、51（第5行第1列），输入者如果不知道偏移的方向或者偏移量就会直接输入：eequ，而用户此次登陆的真实序列应为：11(第1行不变，第5列向右循环移动1列)、12(第1行不变，第5列向右循环移动2列)、45(第4行不变，第2列向右循环移动3列)、55(第5行不变，第1列向右循环移动4列)。由此可知该客户此次登陆的密码应该为：abty。同样也可以左移。

当移动设定为以列为基础向上循环偏移量1、2、3、4；生成的密码为：abty，动态密码装置则提示用户输入索引符号序列为：21（第2行第1列）、32（第3行第2列）、25（第2行第5列）、45（第4行第5列），输入者如果不知道偏移的方向或者偏移量就会直接输入：f1jt，而用户此次登录的真实序列应为：11(第2行向上循环移动1行，第1列不变)、12(第3行向上循环移动2行，第2列不变)、45(第2行向上循环移动3行，第5列不变)、55(第4行向上循环移动4行，第5列不变)。由此可知该客户此次登陆的密码应该为：abty。采用同样的方法也可以向下循环移动。

如图4所示，对于众多的面向内部职工的应用系统来说，采用本发明独立的动态密码系统对内部的所有应用系统的身份认证进行改造，采用这种成本相对较低的方案，即可解决内部单点登录的身份认证的问题。在企业内部使用时动态密码装置可以按照事件驱动的方式产生不同的动态密码，用户端动态密码卡上的索引符号可以采用字母或者其他的任意符号，只是起到索引的作用，而密码符号的取值也是不受限制的，在同一张密码卡上采用的密码符号的种类（字母，标点等其他符号）越多越安全，用户输入终端可以为联上网络的计算机，也可以是交易服务方提供的其他平台，如ATM等。

本发明的有益效果在于，省去了现有动态密码系统中用户端的密码计算器，降低了成本并且保证了相当的安全性，密码系统算法多样性强，更加符合用的需求。

以上具体实施方式仅用于说明本发明，而非用于限定本发明。

卡号：CA1234567890

密码	e	u	j	8	u	6	h	p	w	d	2	u	i	q	q	p	m	x	h
索引序列	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19

图1

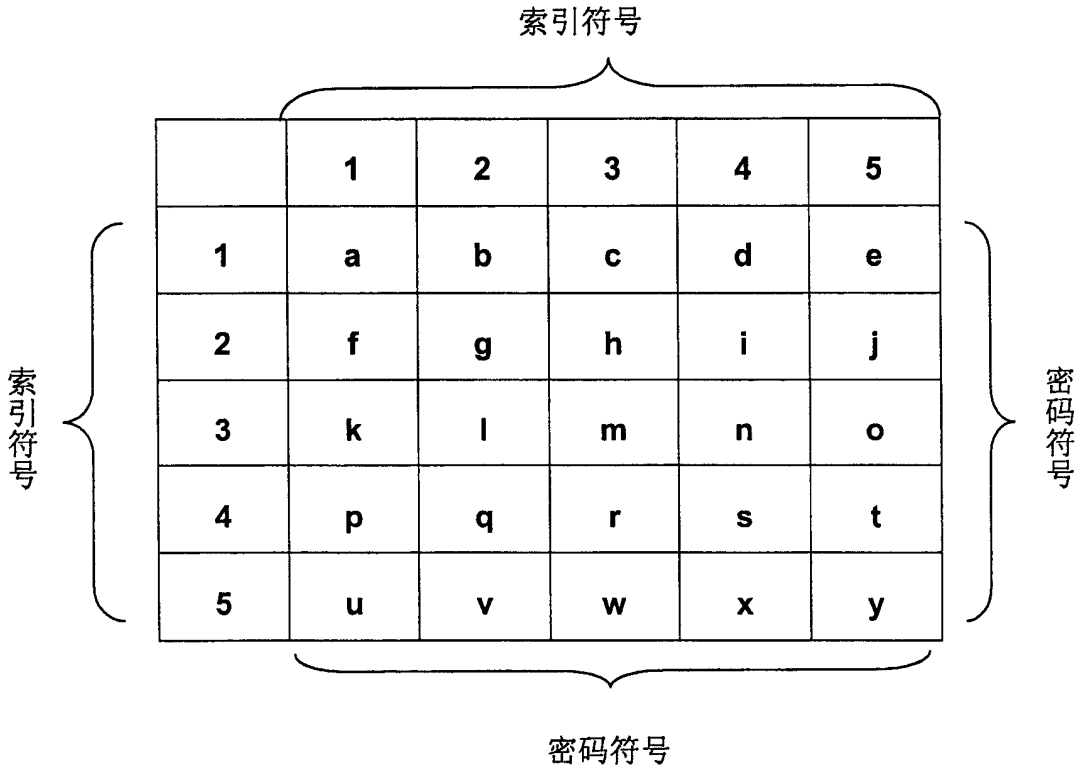


图2

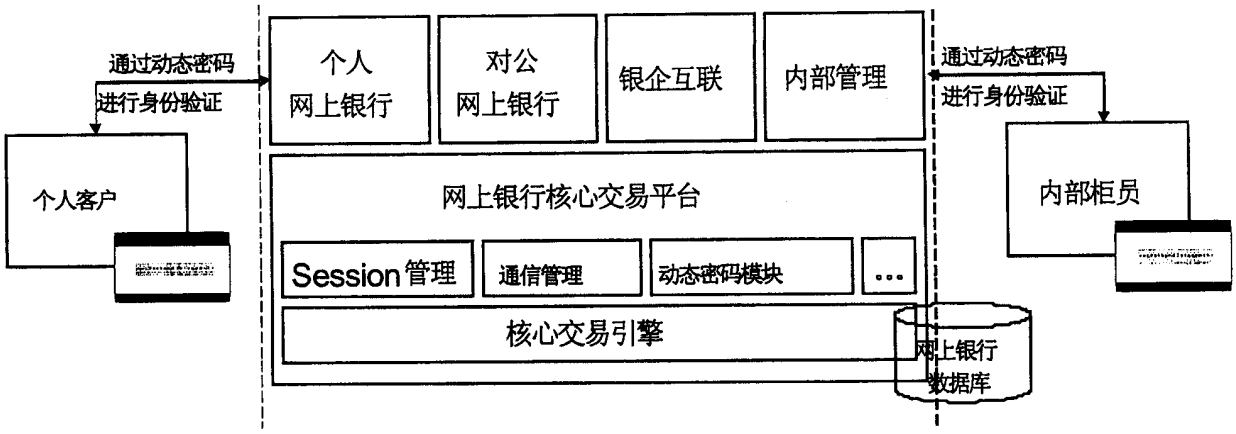

通过动态密码
进行身份验证
个人客户
个人
网上银行
对公
网上银行
银企互联
内部管理
网上银行核心交易平台
Session管理
通信管理
动态密码模块
...
核心交易引擎
网上银行
数据库
通过动态密码
进行身份验证
内部柜员

图3

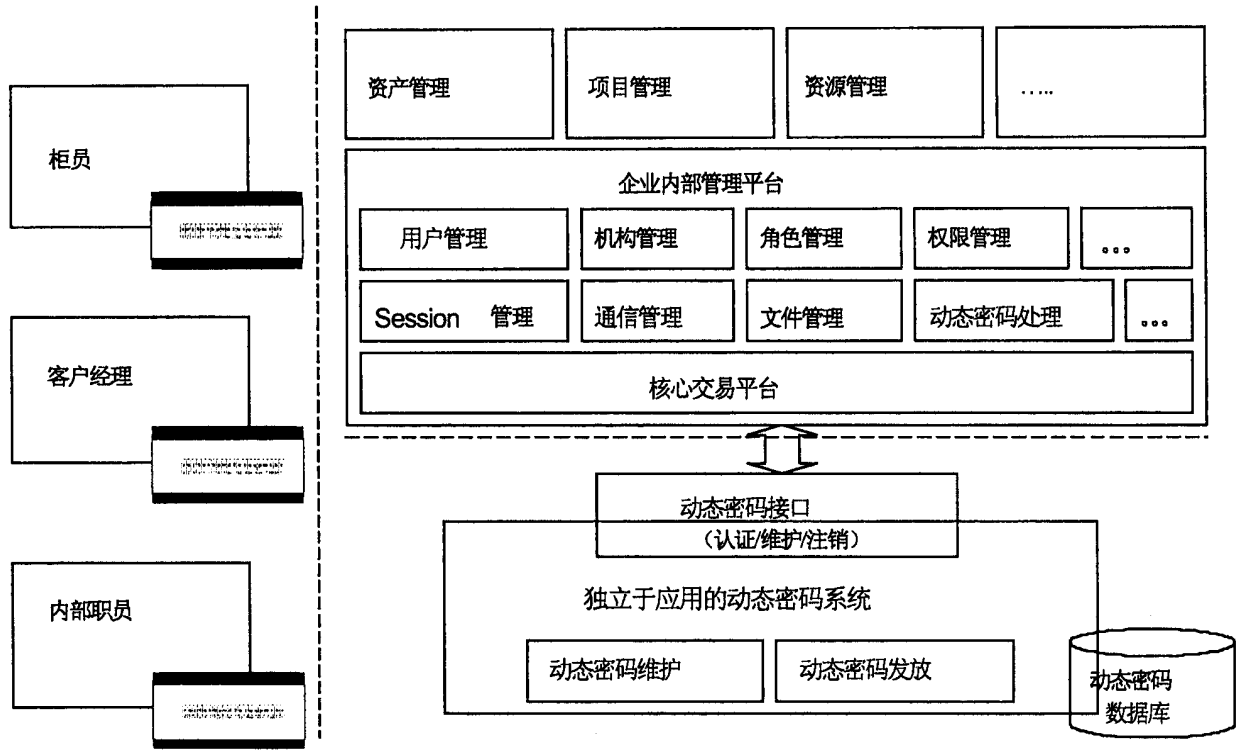

柜员
客户经理
内部职员
资产管理
项目管理
资源管理
.....
企业内部管理平台
用户管理
机构管理
角色管理
权限管理
...
Session 管理
通信管理
文件管理
动态密码处理
...
核心交易平台
动态密码接口
（认证/维护/注销）
独立于应用的动态密码系统
动态密码维护
动态密码发放
动态密码
数据库

图4

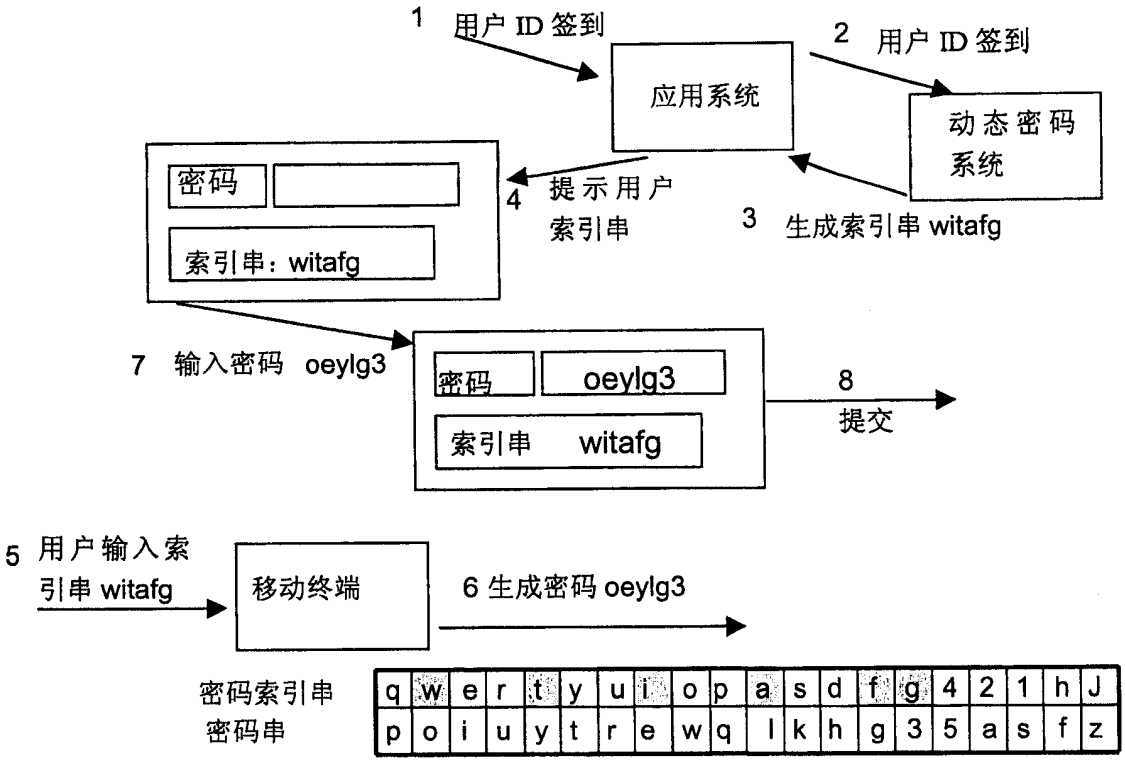

1 用户 ID 签到
2 用户 ID 签到
应用系统
动态密码系统
密码
索引串：witafg
4 提示用户索引串
3 生成索引串 witafg
7 输入密码 oeylg3
密码 oeylg3
索引串 witafg
8 提交
5 用户输入索引串 witafg
移动终端
6 生成密码 oeylg3
密码索引串
密码串
q w e r t y u i o p a s d f g 4 2 1 h J
p o i u y t r e w q l k h g 3 5 a s f z

图5