[19]中华人民共和国国家知识产权局

[51]Int. Cl[7]
G06F 17/60
G06F 13/00

[12]发明专利申请公开说明书

[21]申请号 00109820.9

[43]公开日 2002年1月23日

[11]公开号 CN 1332425A

[22]申请日 2000.7.10 [21]申请号 00109820.9

[71]申请人 黄金富

地址 100055 北京市宣武区广安门外南滨河路1号高新大厦1107室

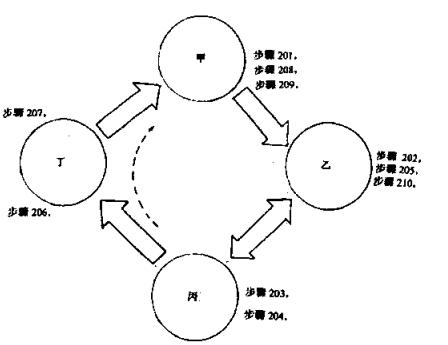
[72]发明人 黄金富

权利要求书2页 说明书5页 附图页数2页

[54]发明名称 采用动态密码的认证付款的方法和相应的电子装置

[57]摘要

一种互连网上确认用户身份和安全支付的方法及相应装置，由动态密码认证 装置(丙)经转发中心(丁)向用户(甲)和直接向商户或银行(乙)发出一随 机产生的同一天码，用户(甲)向商户或银行(乙)输入上述天码和商户或银行 事先给予用户(甲)的心码共同组成的动态密码，供商户或银行进行核对，动态 密码正确，身份确认，交易进行，动态密码认证装置中设有随机码发生器发出动 态天码，本方法确保网上用户身份确认和网上银款支付安全。



ISSN1008-4274

知识产权出版社出版

权利要求

1. 一种在商务中采用电讯方式确认用户身份和安全进行钱款支付的认证方法，其特征在于，由动态密码认证装置（丙）经转发中心（丁）向用户（甲）和直接向商户或银行（乙）发出一随机动态产生的同一天码的密码，用户（甲）向商户或银行（乙）输入包括有所收到的上述天码和商户或银行（乙）事先给予用户（甲）的固定密码的心码共同组合而成的动态密码，供商户或银行（乙）进行核对，动态密码正确，身份确认，交易进行，动态密码不正确，身份不被确认，交易不进行。

2. 如权利要求 1 所述的方法，其特征在于包括如下步骤：

步骤 201，用户（甲）向商户或银行（乙）提出使用动态密码电子认证；

步骤 202，商户或银行（乙）向动态密码认证装置（丙）发出提供动态密码电子认证服务的要求；

步骤 203，动态密码认证装置（丙）产生动态密码的天码；

步骤 204，动态密码认证装置（丙）向商户或银行（乙）及用户（甲）所通过的转发中心（丁）发出上述同一天码的密码；

步骤 205，商户或银行（乙）接收上述天码；

步骤 206，转发中心（丁）接收上述天码；

步骤 207，转发中心（丁）向用户（甲）发出上述天码；

步骤 208，用户（甲）接收上述天码；

步骤 209，用户（甲）发出上述天码和固定密码合成的密码给商户或银行（乙）；

步骤 210，商户或银行（乙）将用户（甲）输入的合成的密码进行核对，对用户（甲）身份进行认证，以确定用户（甲）身份的真伪。

3. 如权利要求 1 或 2 所述的方法，其特征是，动态密码认证装置（丙）向用户（甲）发出随机动态密码的天码所经过的转发中心（丁）可以包括有移动电话中心，有线电话中心，寻呼机中心或电脑因特网中心。

4. 一种在商务中采用电讯方式确认用户身份和安全进行钱款支付的认证装置，称为动态密码认证装置 ，主要包括有输入输出接口（101），中央处理器 CPU

（102），存储器（106），特别是，还包括有随机码发生器（103），客户代码存储器（104），客户邮出地址存储器（105），其中，以中央处理器 CPU（102）为中心，与其它各部分相连接，CPU 按预定程序控制整个装置的作业，随机码发生器（103）产生随机码，并经输入输出接口（101）输出出去，客户邮出地址存储器（105）中存储有所登记的用户所指定的转发地址。

5. 如权利要求 4 所述的认证装置，其特征是，其随机码发生器（103）可以是普来杜随机码发生器（Pseudo Random Number Generator）。

6. 如权利要求 4 所述的认证装置，其特征是，其客户邮出地址存储器（105）中存储的登记用户所指定的转发地址可以是移动电话中心和该用户的姓名或代码或手机号码；

可以是有线电话中心和该用户的姓名或代码或电话号码；

可以是寻呼中心和该用户的姓名或代码或寻呼号码；

可以是因特网中心和该用户的姓名或代码或因特网地址；

说 明 书

采用动态密码的认证付款的方法和相应的电子装置

本发明涉及电讯业，特别是涉及贸易及电子商务中采用动态密码的认识付款方法和装置。

商业活动涉及付款问题，不论是以往的旧的商业模式，还是互连网上的所谓BTB，BTC 等的网上交易模式，当采用即时划帐也就是即时付款时，都存在着一个支付双方身份的可靠性问题，无论是在银行，还是在互连网上，目前都采用固定密码的方式，例如用户甲是中国银行的客户，中国银行就会给用户甲一个密码，用户甲在通过电话由中国银行付帐时，就要输入该密码，作为中国银行识别和确认用户甲的身份的唯一标识。用户甲可以按照中国银行规定的程序更改上述用户身份识别码，这种付款即时过帐对用户甲有很大风险，一旦他的作为用户身份识别码的密码被窃，随时会有钱款损失的危险。因此，更安全的付款方法和相应装置是十分需要的。

本发明的目的，在于提供一种比固定密码方式更安全的采用电讯方式确认用户身份的方法和相应装置。

本发明的目的是这样实现的，即，采用一种在商务中采用电讯方式确认用户身份和安全进行钱款支付的认证方法，其特征在于，由动态密码认证装置（丙）经转发中心（丁）向用户（甲）和直接向商户或银行（乙）发出一随机动态产生的同一天码的密码，用户（甲）向商户或银行（乙）输入包括有所收到的上述天码和商户或银行（乙）事先给予用户（甲）的固定密码的心码共同组合而成的动态密码，供商户或银行（乙）进行核对，动态密码正确，身份确认，交易进行，动态密码不正确，身份不确认，交易不进行，这种方法就是实现本发明的方法，以及，采用一种在商务中采用电讯方式确认用户身份和安全进行钱款支付的认证装置，可称为动态密码认证装置，主要包括有输入输出接口（101），中央处理器CPU（102），存储器（106）特别是还包括有随机码发生器（103），客户代码存储器（104），客户邮出地址存储器（105），其中，以中央处理器 CPU（102）为

中心，与其它各部分相连接，CPU 按预定程序控制整个装置的作业，随机码发生器（103）产生随机码，并经输入输出接口（101）输出出去，客户邮出地址存储器（105）中存储有所登记的用户所指定的转发地址，这样的装置就是实现本发明的装置。

本发明包括如下附图，

图 1 是本发明的动态密码认证装置的结构方框说明图；

图 2 是本发明的动态密码认证方法的流程和步骤说明图；

图 3 是本发明的动态密码认证方法和装置所涉及的通讯网络说明图；

图 4 是本发明的动态密码认证方法和装置所涉及的动态密码构成说明图；

下面结合附图，对本发明作进一步详细说明。

参阅图 1，图 1 是本发明的动态密码认证装置的结构方框说明图，所述装置主要包括有输入输出接口（101），中央处理器即 CPU（102），存储器（106），特别是，还包括有随机码发生器（103），客户代码储器（104），客户邮出地址存储器（105），其中，以 CPU（102）为中心与其它各单元相连接，CPU（102）对整个装置按预定程序进行程序控制，随机码发生器（103）用于产生随机码，该随机码作为用户需要输入的“天码”和银行商户电脑进行用户身份校核的动态密码的组成部分，随机码发生器（103）有多种售品可供选用，例如有普来杜随机码发生器（Pseudo Random Number Generator）等等，它按其预定程式可不断地产生随机码，该随机码很难破译，随机码发生器（103）也可以采用几台不同程式的并联使用等等，使本发明的装置发出的随机码的保密程度大为提高。使用本认证装置的用户的名称地址等资料以代码形式存入客户代码存储器（104）中，每个用户的天码的发送途径的资料存入客户邮出地址存储器（105），例如，用户要求将天码通过他所登记的移动电话公司的电讯系统传给他的手机之类的资料，这类所登记的用户所指定的转发地址存入客户邮出地址存储器（105）中，存储器（106）对提出 认证要求的有关用户资料进行暂存，输入输出接口（101）进行用户要求等的输入和动态随机码的天码的输出。

参阅图 2，图中所示出的是本发明的动态密码认证方法的流程图，其中，甲代表用户，乙代表商户或银行，丙代表电子化的动态密码认证装置，丁代表接收

天码和向用户发出天码的网络中心，或是寻呼机中心，或是移动通信中心，或是有线电话局，简称转发中心（丁），都是相关的电子转发装置，用箭头示出了流程的方向，用 201 至 210 的数字表示出本方法的步骤，步骤从 201 开始，用户（甲）向进行商业活动的商户或银行（乙）提出要求使用动态密码的确认用户身份的本发明的电子方式的认证服务即动态密码电子认证，之后进入步骤 202，收到要求的商户或银行（乙）向动态密码认证装置（丙）发出提供动态密码电子认证服务的要求，进入步骤 203，动态密码认证装置（丙）根据要求及预设程序产生动态密码的天码，之后，进入步骤 204，动态密码认证装置（丙）向两个方向发出天码，一个是向提出要求的商户或银行（乙）发出天码，供商户或银行（乙）认证时核对，步骤 205 是商户或银行（乙）收到天码，另一个方向是向转发中心（丁）发出用户代号和相随的天码，进入步骤 206，转发中心（丁）接收天码，之后，进入步骤 207，由转发中心（丁）向作为它的客户的该用户转发天码，之后，进入步骤 208，用户（甲）收到天码，如果转发中心是手机机站，用户（甲）就用手机收到天码，如转发中心是寻呼机站，用户（甲）就会由其寻呼机上收到天码，以此类推，进入步骤 209，用户（甲）采用商定的电子输入手段按键输入天码和固定密码（可称为常记在心中的心码）的心码，合成的动态密码输给正在等待认证的商户或银行（乙），进入步骤 210，商户或银行（乙）将用户（甲）输入的天码心码的合成的动态密码进行核对，核对无误，身份确认，交易继续进行，天码心码的合成的动态密码如果不正确，则交易对方身份不能确认，交易行为中止，免受损失。

转发中心（丁）起转发作用，本流程中的最主要三方是甲乙丙三方，因此，用虚线示出了从丙到甲的天码输送过程。

采用动态的天码，加上固定的心码，组成合成的动态密码，这个密码会随时不同，随客户不同而不同，因此，采用这种方法，交易各方身份的确认就十分可靠。

综上所述，本发明的动态密码认证付款的方法包括如下步骤：

步骤 201，用户（甲）向商户或银行（乙）提出使用动态密码电子认证；

步骤 202，商户或银行（乙）向动态密码认证装置（丙）发出提供动态密码

电子认证服务的要求；

步骤 203，动态密码认证装置（丙）产生动态密码的天码；

步骤 204，动态密码认证装置（丙）向商户或银行（乙）及用户（甲）所通过的转发中心（丁）发出上述同一天码的密码；

步骤 205，商户或银行（乙）接收上述天码；

步骤 206，转发中心（丁）接收上述天码；

步骤 207，转发中心（丁）向用户（甲）发出上述天码；

步骤 208，用户（甲）接收上述天码；

步骤 209，用户（甲）发出上述天码和固定密码合成的密码给商户或银行（乙）；

步骤 210，商户或银行（乙）将用户（甲）输入的合成的密码进行核对，对用户（甲）身份进行认证，以确定用户（甲）身份的真伪。

本发明的上述方法中所述的动态密码认证装置（丙）向用户（甲）发出随机动态密码的天码所经过的转发中心（丁）可以包括有移动电话中心，有线电话中心，寻呼机中心，或电脑因特网中心。

参阅图 3，图 3 示出的是采用了动态随机码的电子认证所涉及 的通讯网络说明图，网络是以动态密码认证装置（001）为出发点方式示出，为了保密的缘故，通常经电讯专线或专线网络（002）至银行电脑系统（003），银行电脑系统（003）经财经网络或普通电话网络（004）与商户（005）联络。动态密码认证装置（001）发出的动态密码的天码，即经上述途径经专线（002）传给银行电脑（003），或通过普通通讯网络传给提出要求的商户（005），供身份认证的校核之用。另一方面，供商户（005）输入之用的同一天码，是由动态密码认证装置(001)经商户指定的转发中心经通讯网络转发给商户，转发中心可以是有线电话中心（006），有线电话中心（006）根据商户的姓名或代码或电话号码即时将天码转发，经公共电话网（007）传输给该商户的电话（008）或商户的传真机（009），转发中心可以是移动通讯中心（010），移动通讯中心（010）根据商户的姓名或代码或手机电话号码将天码转发，经其移动通讯网（011）传输给该商户的手机（014），转发中心可以是寻呼机中心（013），也是根据商户的姓名或代码或寻呼号码，将天码经移动通讯网传输至商户的寻呼机（012），转发中心可以是因特网

中心（015），也是根据商户的姓名或代号或因特网地址，将天码经因特网（016）传输至该商户的电脑或电子邮箱（017）之类的终端，使该商户（005）马上接收并将天码输入。

参阅图 4，图 4 是本发明的方法和装置所采用和涉及的动态密码的构成的说明图，它由心码加天码构成，心码和天码哪个在先，哪个在后，可以由认证机构或银行等确定，心码一般由银行给客户后，客户可以任意改变，号码可以随时自定，最简单的心码是由一组数字构成，例如 123456 的一组六个数字构成的心码，而天码是由动态密码认证装置所产生和发出，是由其随机码发生器（103）所发出的，例如是前述的普来杜随机码发生器，这些随机码发生器（103）依据一些预定的复杂程式发出随机码，作为天码，最简单的天码也是一级数字，例如 12342234 的一组 8 个数字构成的天码，天码是随机产生，使用时间短暂，它会根据预定程序不断地发出不同的随机的天码，供用户使用。

将心码加天码就得到了动态密码，要由用户输入，要由银行核对，例如上述的心码加天码就是 123456 12342234 的 14 个数字构成的动态密码。

采用了本发明的方法和相应的装置，就可以在不同地区甚至不同国家等等的各种场合，确认对手的身份，由于天码是随时变化的，被他人事后窃走亦无用处，因此本发明的方法和相应装置确保了对用户身份的认证，此方法亦适用于互连网上交易的付款，用户输入动态密码，银行校核动态密码，然后进行支付，转帐等网上银行的业务，可确保用户和银行双方的安全。

本发明的实施，会促进用户和网上银行的安全支付，促进网上商户之间的交易时的身份确认，促进电子商贸的发展。

00.07.10

说　明　书　附　图

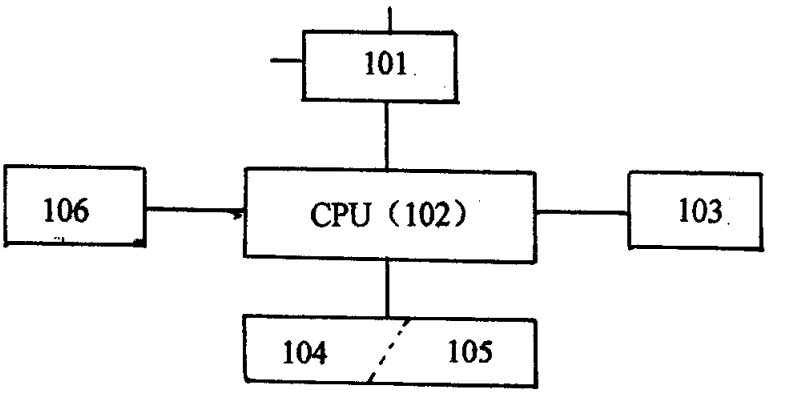


图 1

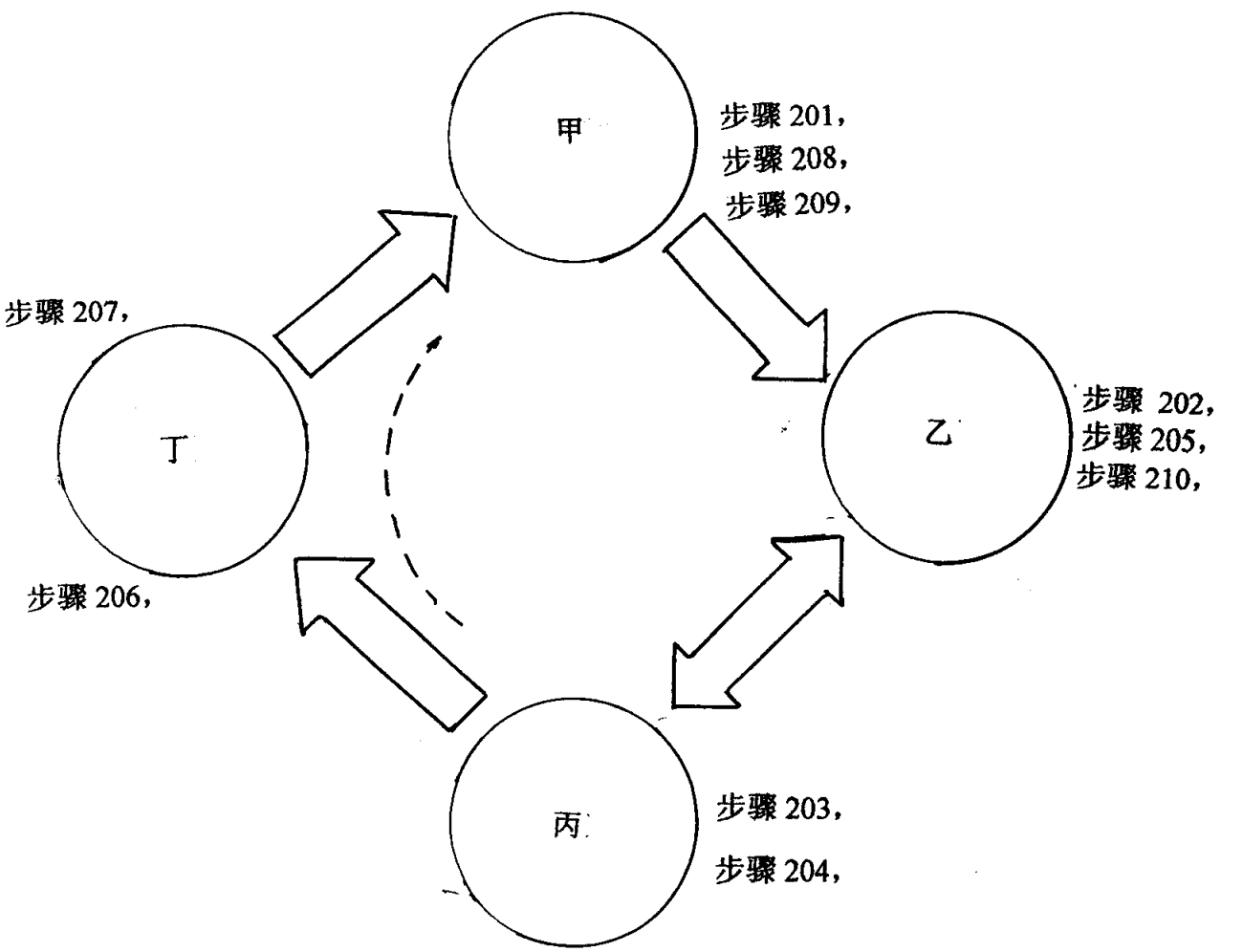


图 2

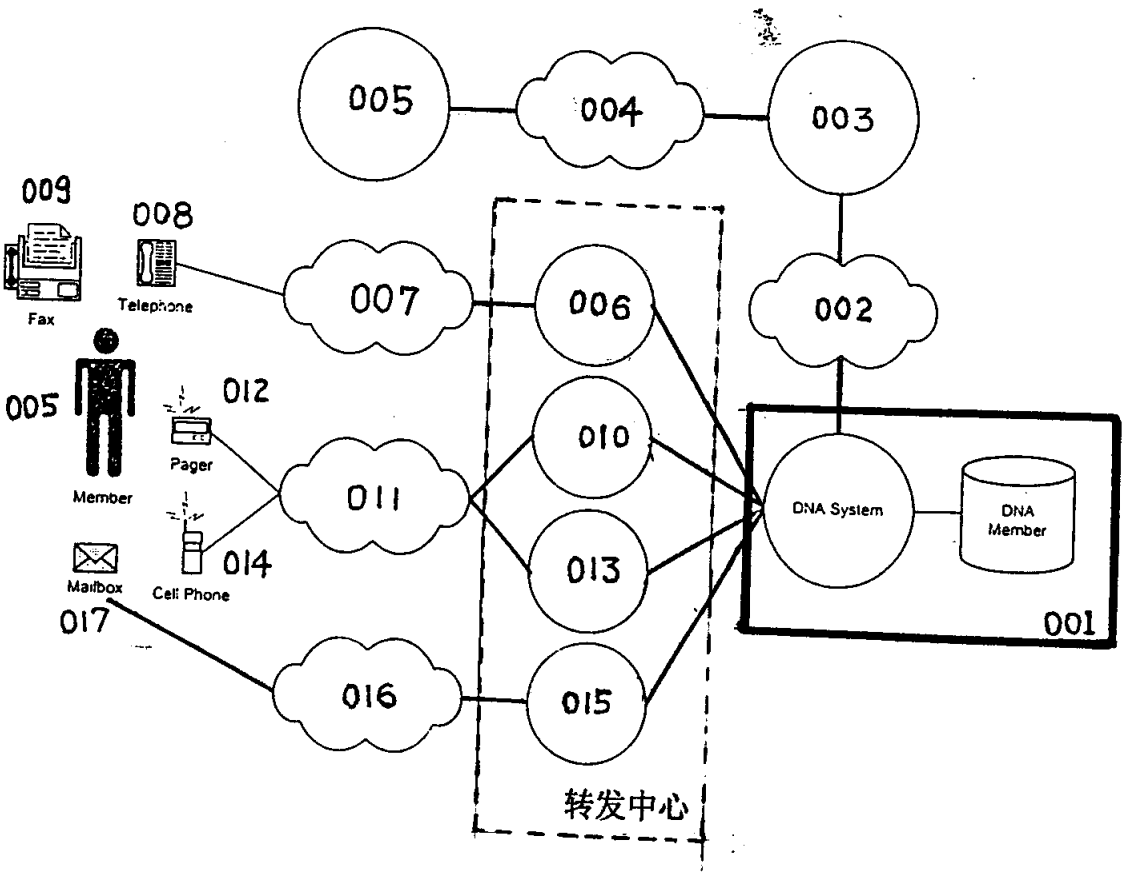

005
004
003
009
008
Fax
Telephone
007
006
002
005
012
010
Pager
011
Member
DNA System
DNA Member
014
013
Cell Phone
Mailbox
017
001
016
015
转发中心

图 3

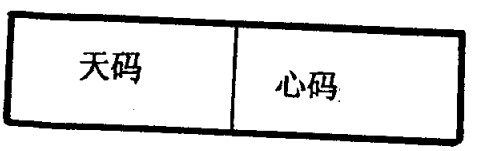

天码
心码

图 4