(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2008 年1 月31 日 (31.01.2008)

PCT

(10) 国际公布号
WO 2008/011758 A1

(51) 国际专利分类号:
H04L 9/32 (2006.01) *G06Q 20/00* (2006.01)
G06F 15/16 (2006.01) *H04L 9/16* (2006.01)

(21) 国际申请号: PCT/CN2006/001787

(22) 国际申请日: 2006 年7 月20 日 (20.07.2006)

(25) 申请语言: 中文

(26) 公布语言: 中文

(71) 申请人及
(72) 发明人: **黄金富(WONG, Kamfu)** [CN/CN]; 中国香港特别行政区湾仔港湾道23号鹰君中心1603室, Hong Kong (CN)。

(74) 代理人: **中国专利代理（香港）有限公司(CHINA PATENT AGENT (H.K.) LTD.)**; 中国香港特别行政区湾仔港湾道23号鹰君中心22号楼, Hong Kong (CN)。

(81) 指定国（除另有指明，要求每一种可提供的国家保护）: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

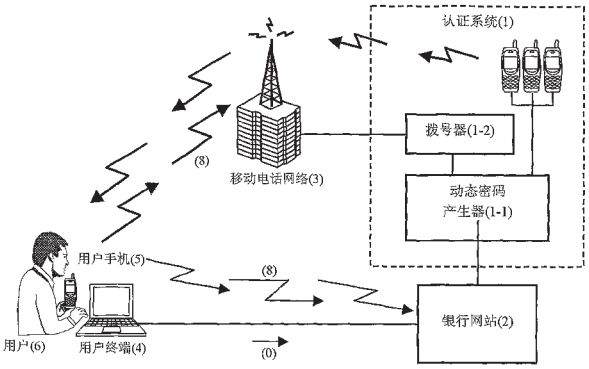
(84) 指定国（除另有指明，要求每一种可提供的地区保护）: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), 欧洲 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)。

本国际公布:
— 包括国际检索报告。

所引用双字母代码及其它缩写符号，请参考刊登在每期PCT公报期刊起始的“代码及缩写符号简要说明”。

(54) Title: METHOD AND SYSTEM FOR ONLINE PAYMENT AND IDENTITY CONFIRMATION WITH SELF-SETTING AUTHENTICATION FORMULA

(54) 发明名称: 网上银钱支付和身份确认的带自设认证算式的方法和系统



1 CERTIFICATION SYSTEM
1-1 DYNAMIC CODE GENERATOR
1-2 DIALER
2 BANK WEBSITE
3 MOBILE TELEPHONE NETWORK
4 USER TERMINAL
5 USER MOBILE TELEPHONE
6 USER

(57) Abstract: A system and a method are used for certification when paying online or confirming the user's identity using the communication network. The system mainly includes a certification system(1), a bank website(2), a mobile telephone network(3), a user terminal and a user mobile telephone and so on. The method includes: the step for certification between the certification system(1) and the user's mobile telephone(5) using the mobile telephone network(3), the step for calculating the certification code(8) using a certification formula(7) defined by the user(6), the step for certification by sending the certification formula(7) defined bythe user(6) to the certification system(1) and storing it therein then calculating the certification code(8) in the certification system(1) or by sending the certification formula(7) defined by the user(6) to the bank website(2) and storing it therein, then calculating the certification code(8) in the bank website(2).

[见续页]

WO 2008/011758 A1

(57) 摘要：

利用电讯网络进行网上银钱支付时或用户身份确认时认证的方法和系统，所述系统主要包括认证系统(1)、银行网站(2)、移动电话网络(3)、用户终端(4)及用户手机(5)等。所述方法包括：

认证系统(1)与用户手机(5)之间通过移动电话网络(3)进行认证的步骤，

用户(6)自定认证算式(7)算出认证密码(8)的步骤，

用户(6)自定认证算式(7)送至并存储在认证系统(1)，认证系统(1)算出认证密码(8)，或用户自定认证算式(7)送至银行网站(2)并存储在银行网站(2)，由银行网站(2)算出认证密码(8)，进行认证的步骤。

网上银钱支付和身份确认的带自设认证算式的方法和系统

技术领域

本发明涉及网上银钱支付的方法和系统，特别是带有随机认证的网上银钱支付的方法和系统。

技术背景

网上银行等网上银钱支付越来越普遍，由于网上购物的流行，网上商业购物、网上个人购物等等，都用到网上银行，或信用卡通过网上支付，利用电讯的网络系统进行支付，甚至包括银行的自动提款机即 ATM 机进行取钱存钱等，也都是利用电讯的网络系统进行的，而网上银钱支付的安全问题是网络支付的头等大事，很多在先专利或专利申请都涉及了这个问题，包括本发明人的在先专利申请 00109820.9 和 01119849.4 号专利申请都提出了用随机动态密码进行网上认证以确保网上安全支付。由于网络业中一些黑客的存在，他们往往利用网络程序中的一些漏洞窃取银行客户各种金融卡客户等银钱支付客户在网上进行业务时的信息，包括窃取随机动态密码，从而对网上安全支付造成一定的威胁，动态密码可能被盗取，银行客户等各种人士利用网上支付可能会造成损失。

因此，更高一级的网上支付认证方法和相应系统是所希望的，即使动态密码被盗取，黑客也不能得逞的方法和系统是需要的，也是急需的。

发明内容

本发明的目的，在于提供一种更新的网上银钱支付的认证方法和相应系统，即使动态密码被盗取，该动态密码不能直接起作用而无法直接被利用，从而确保利用电讯网络的网络支付的安全。本发明的系统也适用于包括银行、信用卡认证、ATM 取款认证等的一切网上支付的情形，本说明书中用银行网站（2）代表各种网上支付机构。

本发明的目的是这样实现的，采用这样一种利用电讯网络进行网上支付时认证的方法，所述方法包括：

认证系统（1）与用户手机（5）之间通过移动电话网络（3）进行认证的步骤，

用户（6）自定认证算式（7）算出认证密码（8）的步骤，

用户（6）自定的认证算式（7）送至并存储在认证系统（1），再由认证系统（1）算出认证密码（8），或用户自定的认证算式（7）送至银行网站（2）并存储在银行网站（2），由银行网站（2）算出认证密码（8），进行认证的步骤；

以及，主要包括认证系统（1）、银行网站（2）、移动电话网络（3）、用户终端（4）及用户手机（5）、用户（6）自定的认证算式（7）和认证密码（8）等的电讯网络认证系统。

本发明的特征是，采用了一种另路认证方法，除使用原有网络传送认证资料，更利用移动电话网络作为传送认证资料的第二路径。认证中心使用动态电话号码拨打用户的手机，用户看见手机上来电显示号码的最后面部份就是随机动态密码，并以用户预先设定的认证算式以加减乘除等运算方式计算出认证密码，然后以用户自己的手机拨打

由认证系统主电话号码加上认证密码组成的电话号码到认证系统，认证系统从来电号码知道是用户的来电，所拨打号码的后面部份就是用户的认证密码。即使动态密码被黑客截取了，黑客没有用户自己的算式，就不能计算出认证密码，而且认证密码是必需从用户手机所发出，所以黑客不能通过认证。本发明适合于一切网上支付认证及各种需要认证的应用，包括网上银行认证，信用卡认证，ATM 取款认证，信用卡公司，股票行，文件储存认证，金融机构，网站，个人资料认证。

本发明的重要特点和优点是认证的方法，可改善目前一般只使用密码作为认证的不足，而且充分利用移动电话网络和手机不易作假的特点，使用简单易用成本低的方法实现另路认证，以 GSM 移动电话网络为例，如果有人复制了用户的 SIM 卡，只要他使用插有复制 SIM 卡的手机跟用户的手机同时在移动电话网络上出现，移动电话公司就会立即停止用户的手机电话号码和用户的 SIM 卡，用户要到移动电话公司重新申请一张新 SIM 卡才能继续使用手机电话号码，这种特性令移动电话网络比互联网等更安全可靠。

此外，本发明的主要优点和特点还有：

一、用户自定认证算式，只有用户自己知道，用户收到随机密码后通过认证算式计算出认证密码。而现时一般没有人使用附加算式方式来做确认，一般是将收到的密码或密码机显示的密码，直接输入。这就是本发明的创新性所在。

二、利用来电显示方式传送密码。

三、使用两种不同途径进行认证，其中一种是现时所用的互联网，另一种是移动电话网络。

附图说明

图 1 是本发明的方法和系统的说明图；

具体实施方式

下面结合附图，对本发明的方法和系统作进一步详细说明。

所述附图和附图说明都是示意性的，本发明的精神不受实施例中的具体说明所限制。

参阅图 1，图 1 中示出了本发明的系统，本发明的电讯网络认证系统主要包括：

认证系统（1），是一包括有电脑的通讯装置，主要包括随机动态密码产生器（1-1）和拨号器（1-2），随机动态密码产生器（1-1）为一电脑服务器，内安装有随机密码产生程序，按预定程序产生指定长度的随机数字符串密码；拨号器（1-2）为电话交换机装置，直接与移动电话网络连接或者通过固定电话网络连接，使用由移动电话网络或固定电话网络商所提供的电话号码的线路，可按预定程序拨打用户的手机电话号码；也可以按预定程序将随机动态密码用短信 SMS 或 MMS 发送给用户；

银行网站（2），是各金融机构的网上交易网站，或者需要认证用户身份的网站；

移动电话网络（3），是一般的移动电话网络，例如 GSM 网络、CDMA 网络等；

用户终端（4），通常为电脑，或各种能上网进行网上支付的电子装置，

用户手机（5），

认证算式（7），由用户（6）自定和用其算出认证密码（8），由用户将自定的认证算式（7）送至并存储在认证系统（1），再由认证系统（1）算出认证密码（8），或用户将自定的认证算式（7）送至银行网站（2）并存储在银行网站（2），由银行网站（2）算出认证密码（8），进行认证。

利用上述本发明的系统，可以采用数种不同的步骤实现本发明的目的。

本发明的第一组方法包括由 A1 至 A8 的 A 组步骤，具体是：

A1. 用户（6）预先到认证系统（1）设定自定的认证算式（7）并存储在认证系统（1），由认证系统（1）其后算出认证密码（8），进行认证；

A2. 用户(6)使用用户终端(4)上网到银行网站(2)，输入登录帐号及密码(0)到银行网站（2）；

A3. 银行网站（2）核对用户（6）的登录帐号及密码无误后，从用户(6)的登录帐号找到用户的手机(5)号码，将用户的手机(5)号码传送给认证系统(1)；

A4. 认证系统(1)通过动态密码产生器(1-1)，产生一个 N 位数字的随机动态密码，然后通过拨号器(1-2)，以认证系统(1)的主电

话号码加上随机动态密码组成的一个电话号码的电话线路，拨打用户的手机(5)号码，拨通后立即挂线；

A5. 用户(6)从手机(5)的来电显示号码，看见是认证系统(1)的来电，知道来电号码的最后面 N 位数字就是随机动态密码，然后以用户预先设定的认证算式（7）计算出认证密码（8）；

A6. 用户（6）将认证密码（8）的 N 位数字替换刚才认证系统（1）的来电号码最后面的 N 位数字组成一个包括认证密码（8）的认证电话号码，使用用户的手机（5）将该认证电话号码拨向认证系统（1），拨通后立即挂线；

A7. 认证系统（1）收到用户（6）的来电，根据用户手机（5）来电号码在认证系统（1）的记录中找到在步骤 A4 中所拨打给用户手机（5）号码及随机密码，将随机密码按用户在步骤 A1 中设定的认证算式（7）计算出认证密码（8）及认证电话号码，只要这认证电话号码与用户手机所拨打的认证电话号码相同就认证成功；

A8. 认证成功后，认证系统（1）通知银行网站（2），刚才银行网站（2）在步骤 A3 所发出的手机（5）号码已经认证成功，银行网站（2）可以让用户（6）正式登录。

其中，上述步骤 A4、A5、A6 中的 N 位数字的 N 为正整数，优选为 6 或 7 或 8。

本发明中的认证系统（1）具有极其独特的性质，就像人体的 DNA 基因那样独特，因而，本发明的系统中的认证系统（1）也可以称为

DNA认证系统。

为了在通讯的电话号码方面实现本发明，首先要由 DNA 认证系统向移动电话公司或固定电话网络公司申请多条电话线路及多个电话号码，例如申请 100 条电话线路及 1,000,000 个电话号码，利用电话号码最后面的 6 位数字，不一定是 6 位，也可以其它码长，即上述 N 位数字作为密码(例如 95599-XXXXXX)，电话号码可以采用延伸方式，将一般的使用电话号码最后面多加几位数字，从而达到增加可用号码目的；以香港电话号码为例，香港电话号码为 8 位数字，只要将号码增加 3 位数字，就可大幅增加可用号码 1,000 倍，例如向电话公司申请一组以固定 5 位数字开始的电话号码，共占用 1,000 个 8 位数字的电话号码，如果将电话号码增加 5 位数字变成 11 位数字电话号码，这样全部可用的电话号码就达到 1,000,000 个。例如以固定 5 位数字 31000 开始的电话号码为 31000XXXXXX，可用号码由 31000000000 至 31000999999，共 1,000,000 个电话号码，最前面 5 位数字取为固定的，也就是作为 DNA 认证系统（1）的所谓主电话号码，用户只要看见所有以这 5 位数字开始的来电号码，就知道是 DNA 认证系统（1）所拨出的电话。

用户（6）同时要在网站登记自己的手机电话号码及设定网上银行（2）登录帐号和密码，并自行设定一组认证算式（7），认证算式（7）由用户自己设定，可以是一些加、减、乘、除、移位运算的算式，计算方法由用户自己定义。

以上说明适用于本发明中的各组方法，包括下述的 B 组步骤和 C

组步骤所说明的方法。

上述步骤 A5 中，例如用户（6）设定的认证算式（7）是：(随机动态密码 + 1968)/12–8,忽略答案中的小数点，即取最前面的 6 个数字就是认证密码（8）。

例如，用户（6）从手机（5）上看到认证系统(1)的来电号码是 31000546382，用户（6）知道最后面 6 位数字 546382 就是随机密码，

则认证算式计算为：(546382 + 1968) / 12 – 8＝45687.833333；

忽略答案 45687.833333 中的小数点，即取答案 45687.833333 最前面的 6 个数字 456878 就是认证密码（8）。

另外，以上步骤还可增加步骤 A9，即：

A9.当用户（6）进行大金额交易操作时，银行网站（2）可以再次要求用户进行认证，以保障用户的帐户安全。

大金额交易中的大金额的数额可由各银行、金融机构和用户（8）根据具体实际情况自行确定。

本发明的方法的第二组实施例的具体步骤由下面的 B1 至 B8 步骤组成，具体说明如下：

B1. 用户（6）预先到银行设定自定的认证算式（7）并存储在银行网站(2)，由银行网站(2)其后算出认证密码（8），进行认证；

B2.用户(6)使用用户终端(4)上网到银行网站(2)，输入登录帐号及密码(0)到银行网站(2)；

B3. 银行网站（2）核对用户（6）的登录帐号及密码无误后，从用户(6)的登录帐号找到用户的手机(5)号码，将用户的手机(5)号码传送给认证系统(1)；

B4. 认证系统(1)通过动态密码产生器(1-1)，产生一个 N 位数字的随机动态密码，然后以下其中的一种方式将随机动态密码传送给用户：

B41、通过拨号器（1-2），以认证系统（1）的主电话号码加上随机动态密码组成的一个电话号码的电话线路，拨打用户（6）的手机（5）号码，拨通后立即挂线；或

B42、认证系统（1）通过短信，将随机动态密码用短信传送给用户手机（5）；或

B43、认证系统（1）通过 MMS，将随机动态密码用 MMS 传送给用户手机（5）；

同时认证系统（1）将随机动态密码传送给银行网站（2）；

B5. 用户(6)从手机(5)的来电显示号码，看见是认证系统(1)的来电，知道来电号码的最后面 N 位数字就是随机动态密码，或从短信或 MMS 的内容看见随机动态密码；然后以用户（6）预先设定的认证算式（7）计算出认证密码（8）；

B6. 用户（6）将认证密码（8）的 N 位数字输入到银行网站（2）；

B7. 银行网站从步骤 B4 中认证系统（1）传来的随机动态密码，按用户（6）在步骤 B1 中设定的认证算式计算出认证密码（8），

只要这认证密码（8）与用户（6）在步骤 B6 中输入的认证密码相同就认证成功；

B8. 认证成功后，银行网站（2）可以让用户（6）正式登录。

同样地，例如，上述步骤 B5 中，例如用户（6）设定的认证算式（7）是：(随机动态密码 + 1968)/12–8,忽略答案中的小数点，即取最前面的 6 个数字就是认证密码（8）。

例如，用户（6）看到认证系统(1)的来电号码是 31000546382，知道最后面 6 个数字 546382 就是随机密码，

则认证算式计算为：(546382 + 1968) / 12 – 8＝45687.833333；

忽略答案 45687.833333 中的小数点，即取答案 45687.833333 最前面的 6 个数字 456878 就是认证密码（8）。

同样地，还可以增加步骤 B9，即：

B9. 当用户（6）进行大金额交易操作时，银行网站（2）可以再次要求用户进行认证，以保障用户的帐户安全。

本实施例 B 组步骤的更进一步改进是在步骤 B5 中，改进的步骤包括用户（6）收到认证系统（1）的包含随机动态密码号码的来电后，立即用手机（5）拨打该随机动态密码电话号码，拨通后立即挂线，认证系统（1）收到来电后，从来电号码知道是用户（6）的来电，知道用户（6）作了确认，立即将收到的该确认信息传送给银行网站（2），这样可进一步加强认证的安全性。

本发明的第三组步骤的具体步骤由下面的 C1 至 C8 步骤组成，具体说明如下：

C1. 用户（6）预先到认证系统（1）设定自定的认证算式（7）并存储在认证系统（1），由认证系统（1）其后算出认证密码（8），进行认证；

C2.用户(6)使用用户终端(4)上网到银行网站(2)，输入登录帐号及密码(0)到银行网站(2)；

C3. 银行网站（2）核对用户（6）的登录帐号及密码无误后，从用户(6)的登录帐号找到用户的手机(5)号码，将用户的手机(5)号码传送给认证系统(1)；

C4. 认证系统(1)通过动态密码产生器(1-1)，产生一个 N 位数字的随机动态密码，然后通过短信或 MMS，将随机动态密码传送给用户手机（5）；

C5. 用户(6)从短信或 MMS 的来电显示号码，知道是认证系统(1)的所发的短信或 MMS，并从短信或 MMS 的内容看见随机动态密码；然后以用户（6）预先设定的认证算式（7）计算出认证密码（8）；

C6.用户（6）利用其手机（5）将认证密码（8）用短信或 MMS 传回认证系统（1）；

C7. 认证系统（1）收到用户（6）用其手机（5）发回的认证密码（8），根据用户手机（5）来电号码在认证系统（1）的记录中找到在步骤 C4 中所发给用户（6）的随机动态密码，将随机动态密码按用户（6）在步骤 C1 中设定的认证算式（7）计算

出认证密码（8），只要这认证密码（8）与用户手机所发回的认证密码（8）相同就认证成功；

C8. 认证成功后，认证系统（1）通知银行网站（2），刚才银行网站（2）在步骤 C3 所发出的手机（5）号码已经认证成功，银行网站（2）可以让用户（6）正式登录。

和前面的 A 组步骤和 B 组步骤中一样，步骤 C5 中，举同样的例子，说明从认证算式（7）计算出认证密码的情形。

同样地，例如用户（6）设定的认证算式（7）是：(随机动态密码 + 1968)/12–8,忽略答案中的小数点，即取最前面的 6 个数字就是认证密码（8）。

例如，用户（6）看到来电号码是 31000546382，知道最后面 6 位数字 546382 就是随机密码，

则认证算式计算为：(546382 + 1968) / 12 – 8＝45687.833333；

忽略答案 45687.833333 中的小数点，即取答案 45687.833333 最前面的 6 个数字 456878 就是认证密码（8）。

认证算式（7）是用户（6）自己设定的，下面举出更多的用户的认证算式（7）的例子：

例 1：使用六位数字密码，随机密码是 945218：

认证算式（7）是：随机密码×7–111100，

945218×7–111100＝6505426，

取最前面的六数字 650542 就是认证密码（8）；

例 2：使用八位数字密码，随机密码是 54125236，

认证算式（7）是：（随机密码最前面两位数字与最后两位数字对调）×3，

54125236 前面两位数字与最后两位数字对调＝36125254，

36125254×3＝108375762，

取最前面的八个数字 10837576 就是认证密码（8）；

例 3：使用七位数字密码，随机密码是 6589462，

认证算式（7）是：（随机密码第四至六位数字变为 128）×9+1668，

6589462 第四至六位数字变为 128 ＝ 6581282，

6581282×9 +1668＝59233206，

取最前面的七个数字 5923320 就是认证密码（8）；

例 4：使用十位数字密码，随机密码是 9452123176，

认证算式（7）是：（随机密码第七位数字+1 及第八位数字+1），

9452123176 第七位数字+1 及第八位数字+1＝9452124276，

取最前面的十个数字 9452124276 就是认证密码（8）；

随机密码即随机动态密码的长度（位数）可以和认证密码（8）一样长，如本说明书中都取 N 是为了用户记忆方便，也可以不一样长，例如认证密码（8）固定为 6 位，等等，也是可以的，也属于本发明的保护范围。

由于各国的电话网络所使用的电话号码长度不同，可因应需要选择合适长度的动态密码，最理想的长度为 6 至 8 位数字。本发明使用的移动电话网络并不直接与 Internet 互联网络连线，黑客即使使用木马间谍程式，偷了用户（6）的登录密码，由于没有用户（6）的手机（5），也就不能接收 DNA 认证系统的随机动态密码，另外黑客也没

有用户（6）的认证算式（7），就不能通过认证，确保了用户（6）的网上支付的安全。

综上所述，在上述各组步骤最后，可增加第 9 步骤，即：

当用户（6）进行大金额交易操作时，银行网站（2）可以再次要求用户进行认证，以保障用户的帐户安全。

以及，认证密码（8）的算法是，当随机动态密码被经认证算式（7）计算后得出非整数答案时，忽略答案中的小数点，即取答案最前面的 N 个数字就是认证密码（8）。

前面所述中，字母串 MMS 是 Multimedia Messaging Service 的缩写，中文意思为多媒体短信服务。

以及，上面所述的认证方法，其特征在于，该认证方法使用两条不同途径进行认证，其中一条是现时使用的互联网，另一条是移动电话网络（3）。

以及，上面所述的认证方法，其特征在于，随机动态密码和认证密码（8）都利用来电显示方式传送。

以及，上面所述的认证方法，所述方法适用于一切网上支付认证，包括网上银行认证，信用卡认证，ATM 取款认证，也包括了用户的身份认证，私人信贷资料库的认证，网站，个人资料认证，金融机构认证，文件储存认证，股票行认证，等等，各种需要认证的应用。

本发明的认证方法的实施，会给银行和用户等各方都带来很好的效果。

权利要求书

1.一种利用电讯网络进行网上支付时和／或身份确认时认证的方法，所述方法包括：

认证系统（1）与用户手机（5）之间通过移动电话网络（3）进行认证的步骤，

用户（6）自定认证算式（7）算出认证密码（8）的步骤，

用户（6）将自定的认证算式（7）送至并存储在认证系统（1），再由认证系统（1）算出认证密码（8），或用户将自定的认证算式（7）送至银行网站（2）并存储在银行网站（2），由银行网站（2）算出认证密码（8），进行认证的步骤；

2. 如权利要求 1 所述的认证方法，所述方法包括如下 A 组步骤：

A1. 用户（6）预先到认证系统（1）设定自定的认证算式（7）并存储在认证系统（1），由认证系统（1）其后算出认证密码（8），进行认证；

A2. 用户(6)使用用户终端(4)上网到银行网站(2)，输入登录帐号及密码(0)到银行网站（2）；

A3. 银行网站（2）核对用户（6）的登录帐号及密码无误后，从用户(6)的登录帐号找到用户的手机(5)号码，将用户的手机(5)号码传送给认证系统(1)；

A4. 认证系统(1)通过动态密码产生器(1-1)，产生一个 N 位数字的随机动态密码，然后通过拨号器(1-2)，以认证系统(1)的主电

话号码加上随机动态密码组成的一个电话号码的电话线路，拨打用户的手机(5)号码，拨通后立即挂线；

A5. 用户(6)从手机(5)的来电显示号码，看见是认证系统(1)的来电，知道来电号码的最后面 N 位数字就是随机动态密码，然后以用户预先设定的认证算式（7）计算出认证密码（8）；

A6. 用户（6）将认证密码（8）的 N 位数字替换刚才认证系统（1）的来电号码最后面的 N 位数字组成一个包括认证密码（8）的认证电话号码，使用用户的手机（5）将该认证电话号码拨向认证系统（1），拨通后立即挂线；

A7. 认证系统（1）收到用户（6）的来电，根据用户手机（5）来电号码在认证系统（1）的记录中找到在步骤 A4 中所拨打给用户手机（5）号码及随机密码，将随机密码按用户在步骤 A1 中设定的认证算式（7）计算出认证密码（8）及认证电话号码，只要这认证电话号码与用户手机所拨打的认证电话号码相同就认证成功；

A8. 认证成功后，认证系统（1）通知银行网站（2），刚才银行网站（2）在步骤 A3 所发出的手机（5）号码已经认证成功，银行网站（2）可以让用户（6）正式登录。

3. 如权利要求 1 所述的认证方法，所述方法包括如下 B 组步骤：

B1. 用户（6）预先到银行设定自定的认证算式（7）并存储在银行网站(2)，由银行网站(2)其后算出认证密码（8），进行认证；

B2. 用户(6)使用用户终端(4)上网到银行网站(2)，输入登录帐号及密码(0)到银行网站(2)；

B3. 银行网站（2）核对用户（6）的登录帐号及密码无误后，从用户(6)的登录帐号找到用户的手机(5)号码，将用户的手机(5)号码传送给认证系统(1)；

B4. 认证系统(1)通过动态密码产生器(1-1)，产生一个 N 位数字的随机动态密码，然后以下其中的一种方式将随机动态密码传送给用户：

B41、通过拨号器（1-2），以认证系统（1）的主电话号码加上随机动态密码组成的一个电话号码的电话线路，拨打用户（6）的手机（5）号码，拨通后立即挂线；或

B42、认证系统（1）通过短信，将随机动态密码用短信传送给用户手机（5）；或

B43、认证系统（1）通过 MMS，将随机动态密码用 MMS 传送给用户手机（5）；

同时认证系统（1）将随机动态密码传送给银行网站（2）；

B5. 用户(6)从手机(5)的来电显示号码，看见是认证系统(1)的来电，知道来电号码的最后面 N 位数字就是随机动态密码，或从短信或 MMS 的内容看见随机动态密码；然后以用户（6）预先设定的认证算式（7）计算出认证密码（8）；

B6. 用户（6）将认证密码（8）的 N 位数字输入到银行网站（2）；

B7. 银行网站从步骤 B4 中认证系统（1）传来的随机动态密码，按用户（6）在步骤 B1 中设定的认证算式计算出认证密码（8），只要这认证密码（8）与用户（6）在步骤 B6 中输入的认证密码相同就认证成功；

B8. 认证成功后，银行网站（2）可以让用户（6）正式登录。

4. 如权利要求 1 所述的认证方法，所述方法包括如下 C 组步骤：

C1. 用户（6）预先到认证系统（1）设定自定的认证算式（7）并存储在认证系统（1），由认证系统（1）其后算出认证密码（8），进行认证；

C2. 用户(6)使用用户终端(4)上网到银行网站(2)，输入登录帐号及密码(0)到银行网站(2)；

C3. 银行网站（2）核对用户（6）的登录帐号及密码无误后，从用户(6)的登录帐号找到用户的手机(5)号码，将用户的手机(5)号码传送给认证系统(1)；

C4. 认证系统(1)通过动态密码产生器(1-1)，产生一个 N 位数字的随机动态密码，然后通过短信或 MMS，将随机动态密码传送给用户手机（5）；

C5. 用户(6)从短信或 MMS 的来电显示号码，知道是认证系统(1)所发的短信或 MMS，并从短信或 MMS 的内容看见随机动态密码；然后以用户（6）预先设定的认证算式（7）计算出认证密码（8）；

C6. 用户（6）利用其手机（5）将认证密码（8）用短信或 MMS 传回认证系统（1）；

C7. 认证系统（1）收到用户（6）用其手机（5）发回的认证密码（8），根据用户手机（5）来电号码在认证系统（1）的记录中找到在步骤 C4 中所发给用户（6）的随机动态密码，将随机动态密码按用户（6）在步骤 C1 中设定的认证算式（7）计算出认证密码（8），只要这认证密码（8）与用户手机所发回的认证密码（8）相同就认证成功；

C8. 认证成功后，认证系统（1）通知银行网站（2），刚才银行网站（2）在步骤 C3 所发出的手机（5）号码已经认证成功，银行网站（2）可以让用户（6）正式登录。

5. 如权利要求 1 或 2 或 3 或 4 所述的认证方法，当用户（6）进行大金额交易操作时，银行网站（2）可以再次要求用户进行认证，以保障用户的帐户安全。

6. 如权利要求 1 或 2 或 3 或 4 所述认证方法，当随机动态密码被经认证算式（7）计算后得出非整数答案时，忽略答案中的小数点，取答案中最前面的 N 个数字就是认证密码（8）。

7. 如权利要求 1 至 6 任一项权利要求所述的认证方法，其特征在于，该认证方法使用两条不同途径进行认证，其中一条是现时使用的互联网，另一条是移动电话网络（3）。

8. 如权利要求 1 或 2 或 3 或 4 或 5 所述认证方法，其特征在于，随机动态密码和认证密码（8）都利用来电显示方式传送。

9. 如权利要求 1 至 8 中任一项所要求的认证方法，所述方法适用于一切网上支付认证及各种需要认证的应用，包括网上银行认证，信用卡认证，ATM 取款认证，信用卡公司，股票行，文件储存认证，金融机构，网站，个人资料认证。

10. 一种利用电讯网络进行网上支付时和／或身份确认时的电讯网络认证系统，所述电讯网络认证系统包括：

认证系统（1），是一包括有电脑的通讯装置，主要包括随机动态密码产生器（1-1）和拨号器（1-2），随机动态密码产生器（1-1）为一电脑服务器，内安装有随机密码产生程序，按预定程序产生指定长度的随机数字符串密码；拨号器（1-2）为电话交换机装置，直接与移动电话网络连接或者通过固定电话网络连接，使用由移动电话网络或固定电话网络商所提供的电话号码的线路，可按预定程序拨打用户的手机电话号码；也可以可按预定程序将随机动态密码用短信 SMS 或 MMS 发送给用户；

银行网站（2），是各金融机构的网上交易网站，或者需要认证用户身份的网站；

移动电话网络（3），是一般的移动电话网络，例如 GSM 网络、CDMA 网络等；

用户终端（4），通常为电脑，或各种能上网进行网上支付的电子装置，

用户手机（5），

认证算式（7），由用户（6）自定和用其算出认证密码（8），由用户

将自定的认证算式（7）送至并存储在认证系统（1），再由认证系统（1）算出认证密码（8），或，用户将自定的认证算式（7）送至银行网站（2）并存储在银行网站（2），由银行网站（2）算出认证密码（8），进行认证。

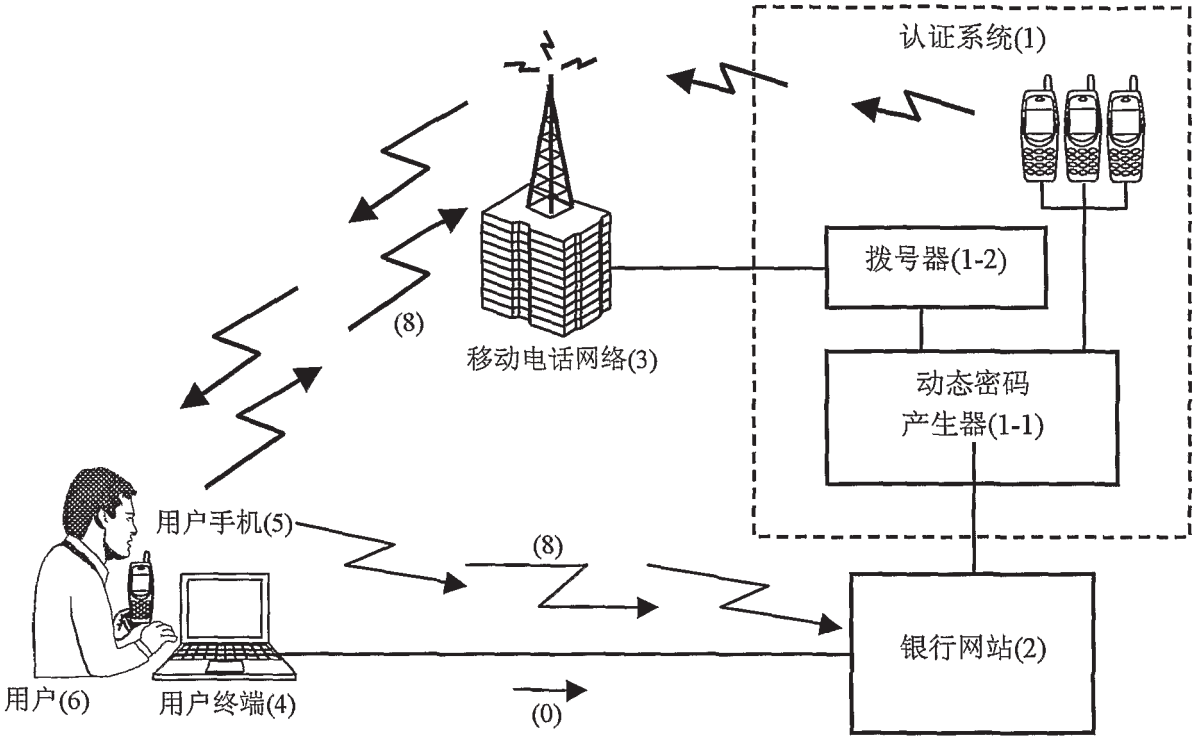


图 1