

(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
2014年9月25日 (25.09.2014)



(10) 国际公布号
WO 2014/146286 A1

- (51) 国际专利分类号:
G06Q 20/00 (2012.01)
- (21) 国际申请号: PCT/CN2013/073030
- (22) 国际申请日: 2013年3月22日 (22.03.2013)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (72) 发明人; 及
- (71) 申请人: 黄凯铃 (WONG, HoiLing) [CN/CN]; 中国香港特别行政区沙田径口路3号金富台, 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香港湾仔港湾道23号鹰君中心22字楼, 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, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR,

CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, 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, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, 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(条约第21条(3))。

(54) Title: SECURE PAYMENT SYSTEM AND METHOD FOR BANK CARD BY USING REAL-TIME COMMUNICATION

(54) 发明名称: 利用实时通讯的银行卡安全支付系统和方法

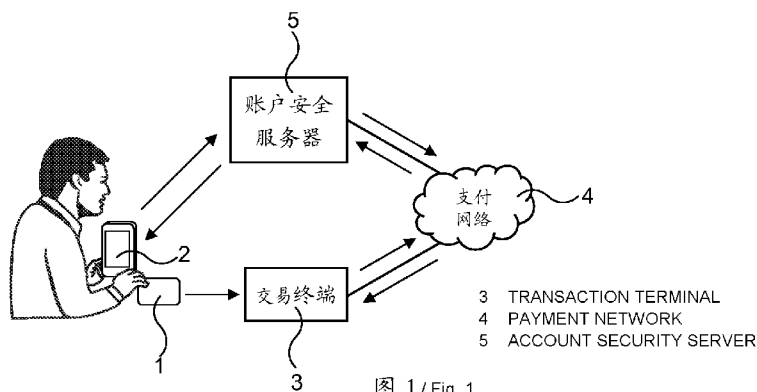


图 1 / Fig. 1

(57) Abstract: A secure payment system and method for a bank card by using real-time communication, comprising a bank card account and a mobile phone (2) of a user, a transaction terminal (3) of a commercial tenant, a payment network (4), and an account security server (5). The account security server (5) is provided with real-time communication server end software. The mobile phone (2) of the user is provided with a real-time communication application pattern. The mobile phone (2) accesses the account security server (5) by using the real-time communication application pattern. The bank card account of the user is associated with the mobile phone (2). When the payment network (4) receives a transaction request transferred by the transaction terminal (3) of the commercial tenant and belonging to the bank card account of the user, the payment network (4) performs, by using the account security server (5) and the mobile phone (2) associated with the bank card account, security verification for verifying an identity of the user in a real-time communication manner, and after the verification succeeds, continues to perform a subsequent step of the transaction; otherwise, refuses the transaction.

(57) 摘要:

[见续页]



WO 2014/146286 A1

一种利用实时通讯的银行卡安全支付系统和方法，包括用户的银行卡账户和手机（2）、商户的交易终端（3）、支付网络（4）、账户安全服务器（5），账户安全服务器（5）设有实时通讯服务器端软件，用户的手机（2）设有实时通讯应用程序，手机（2）通过该实时通讯应用程序接入账户安全服务器（5），用户的银行卡账户与手机（2）相关联。当支付网络（4）收到商户的交易终端（3）传送来属于用户的银行卡账户的交易请求时，支付网络（4）通过账户安全服务器（5）和该银行卡账户相关联的手机（2）以实时通讯方式进行验证该用户身份的安全验证，验证成功后才继续该交易的后续步骤，否则拒绝交易。

利用实时通讯的银行卡安全支付系统和方法

【技术领域】

本发明涉及金融支付领域，特别是涉及一种利用实时通讯的银行卡安全支付系统和方法。

【背景技术】

由于银行卡携带方便，而且容易使用，给卡主带来快捷方便的支付方法，所以银行卡的使用越来越普遍，很多人拥有超过一张银行卡。虽然银行卡给予卡主快捷方便的支付方法，但是也带来一些保安问题，一些犯罪分子通过种种手段盗取他人的银行卡资料，然后复制假卡进行消费付款，或者盗用卡主的银行卡资料在网上消费，卡主一般要收到月结单后才会发觉自己的银行卡账户被人盗用，令卡主蒙受损失，是一个极待解决的问题。为保护银行卡账户安全，防止卡主的银行卡账户被盗用，而提出本发明的利用实时通讯的银行卡安全支付系统和方法。

【发明内容】

本发明的目的，在于提供一种利用实时通讯的银行卡安全支付系统和方法，以实现在安全支付中的多种应用。

本发明的目的是这样实现的，采用这样一种银行卡安全支付系统，其特征在于，所述的系统包括用户的银行卡账户和手机（2）、商户的交易终端（3）、支付网络（4）、账户安全服务器（5），其中，账户安全服务器（5）与支付网络（4）相电讯连接，账户安全服务器（5）设有实时通讯服务器端软件，用户的手机（2）设有实时通讯应用程序，手机（2）通过该实时通讯应用程序经通讯网络例如移动电话网络、WIFI 网络等等无线网络接入账户安全服务器（5），交易终端（3）通过有线/无线网络例

如移动电话网络、WIFI 网络、区域网络、互联网络等等各类网络接入支付网络（4），账户安全服务器（5）记录用户的银行卡账户的账户资料，用户的银行卡账户与该用户的手机（2）相关联，以及，当支付网络（4）收到商户的交易终端（3）传送来属于用户的银行卡账户的交易请求时，支付网络（4）通过账户安全服务器（5）和该银行卡账户相关联的手机（2）进行验证该用户身份的安全验证，安全验证成功后支付网络（4）才继续进行该交易的后续步骤，否则拒绝该交易。

以及，还采用这样一种银行卡安全支付方法，其特征在于，所述的方法包括设置账户安全服务器（5），在账户安全服务器（5）记录用户的银行卡账户的账户资料，并将用户的银行卡账户与该用户的手机（2）相关联，账户安全服务器（5）与支付网络（4）相电讯连接，账户安全服务器（5）设有实时通讯服务器端软件，用户的手机（2）设有实时通讯应用程序，手机（2）通过该实时通讯应用程序经通讯网络例如移动电话网络、WIFI 网络等等无线网络接入账户安全服务器（5），以及，当支付网络（4）收到商户的交易终端（3）传送来属于用户的银行卡账户的交易请求时，支付网络（4）通过账户安全服务器（5）和该银行卡账户的相关联的手机（2）进行验证该用户身份的安全验证，安全验证成功后支付网络（4）才继续进行该交易的后续步骤，否则拒绝该交易。

这样就很好地实现本发明的目的。

本发明的支付系统和方法，在用户支付时，通过实时通讯方式与用户的手机（2）通讯，即时验证用户身份的真确性，以保障用户的银行卡账户安全。此外，账户安全服务器（5）与用户手机（2）之间的实时通讯，是采用独立于原来银行卡支付网络的通讯路径来进行验证用户身份的步骤，所以即使用户的银行卡账户被贼人盗用，只要用户的手机（2）在手，贼人就无法得逞，保障了用户的银行卡账户安全。

【附图说明】

图 1 是本发明第一实施例的银行卡安全支付系统的形像化示意说明图；
图 2 是本发明第二实施例的银行卡安全支付系统的形像化示意说明图；
图 3 是本发明第三实施例的银行卡安全支付系统的形像化示意说明图；
图 4 是本发明第四实施例的银行卡安全支付系统的形像化示意说明图；
图 5 是本发明第五实施例的银行卡安全支付系统的形像化示意说明图；
图 6 是本发明第六实施例的银行卡安全支付系统的形像化示意说明图；
图 7 是本发明第七实施例的银行卡安全支付系统的形像化示意说明图；
图 8 是本发明第八实施例的银行卡安全支付系统的形像化示意说明图。

图中，相同的数字代表相同的系统、装置、部件器件，附图是示意性的，用以说明本发明的构成和主要特征。

【具体实施方式】

下面结合附图，对本发明的方法作进一步详细说明。

参阅图 1，图 1 是本发明第一实施例的银行卡安全支付系统的形像化示意说明图，图 1 中示出的系统包括代表用户的银行卡账户的银行卡（1）和用户的手机（2）、商户的交易终端（3）、支付网络（4）、账户安全服务器（5），其中，账户安全服务器（5）与支付网络（4）相电讯连接，账户安全服务器（5）设有实时通讯服务器端软件，用户的手机（2）设有实时通讯应用程序，手机（2）通过该实时通讯应用程序经通讯网络例如移动电话网络、WIFI 网络等等无线网络接入账户安全服务器（5），商户的交易终端（3）通过有线/无线网络例如移动电话网络、WIFI 网络、区域网络、互联网络等等各类网络接入支付网络（4），用户需要在账户安全服务器（5）登记他的银行卡账户的账户资料和手机（2）资料，账户安全服务器（5）记录用户的银行卡账户的账户资料，将用户的银行卡账户与该用户的手机（2）相关联，以及，用户在商户的交易终

端（3）使用其银行卡账户进行支付，当支付网络（4）收到商户的交易终端（3）传送来属于用户的银行卡账户的交易请求时，支付网络（4）通过账户安全服务器（5）和该银行卡账户相关联的手机（2）进行验证该用户身份的安全验证，安全验证成功后支付网络（4）才继续进行该交易的后续步骤，否则拒绝该交易。在本发明中，是在原有一般的银行卡支付系统中，增加本发明的账户安全服务器（5），并在进行支付时，额外增加安全验证用户身份的步骤，通过这账户安全服务器（5）与用户的手机（2）以实时通讯方式对用户的身份进行安全验证，安全验证成功后，支付网络（4）和商户的交易终端（3）还须要继续执行原来尚未执行的操作，这些操作就是本说明书所述的后续步骤，例如验证用户账户结余、账户信用额等等，由于这些是属于现有银行卡支付应有的操作步骤，这部分并非本发明的特征，所以本说明书不作详细说明。

继续参阅图 1，图 1 中示出的银行卡安全支付系统所采用的方法包括设置账户安全服务器（5），在账户安全服务器（5）记录用户的银行卡账户的账户资料，并将用户的银行卡账户与该用户的手机（2）相关联，账户安全服务器（5）与支付网络（4）相电讯连接，账户安全服务器（5）设有实时通讯服务器端软件，用户的手机（2）设有实时通讯应用程序，手机（2）通过该实时通讯应用程序经通讯网络例如移动电话网络、WIFI 网络等等无线网络接入账户安全服务器（5），以及，当支付网络（4）收到商户的交易终端（3）传送来属于用户的银行卡账户的交易请求时，支付网络（4）通过账户安全服务器（5）和该银行卡账户的关联的手机（2）进行验证该用户身份的安全验证，安全验证成功后支付网络（4）才继续进行该交易的后续步骤，否则拒绝该交易。

参阅图 2 至图 4，图 2 是本发明第二实施例的银行卡安全支付系统的形像化示意说明图，图 3 是本发明第三实施例的银行卡安全支付系统的形像化示意说明图，图 4 是本发明第四实施例的银行卡安全支付系统的形像

化示意说明图，图 2 至图 4 中分别示出了本发明第二至第四实施例，分别示出了采用不同的方式的支付网络（4）来实现本发明的例子，以下对这些不同的实施例子作进一步详细说明。

继续参阅图 2，图 2 示出的第二实施例的支付网络（4）包括银行卡网络（401）、设有商户的银行账户的收单银行（402）、设有用户的银行卡账户的发卡银行（403），其中，银行卡网络（401）分别与收单银行（402）和发卡银行（403）相电讯连接，并与所述的账户安全服务器（5）相电讯连接，交易终端（3）通过有线/无线网络例如移动电话网络、WIFI 网络、区域网络、互联网络等等各类网络接入支付网络（4）的收单银行（402），银行卡网络（401）于处理属于用户的银行卡账户的交易请求时，通过账户安全服务器（5）和该银行卡账户相关联的手机（2）进行验证该用户身份的安全验证。在第二实施例中，账户安全服务器（5）与银行卡网络（401）相电讯连接，可以将账户安全服务器（5）整合于银行卡网络（401）中，所有通过银行卡网络（401）处理的交易支付都可以通过账户安全服务器（5）对用户的身份进行安全验证步骤，从而保障用户的银行卡账户的安全。

继续参阅图 3，图 3 示出的第三实施例的支付网络（4）包括银行卡网络（401）、设有商户的银行账户的收单银行（402）、设有用户的银行卡账户的发卡银行（403），其中，银行卡网络（401）分别与收单银行（402）和发卡银行（403）相电讯连接，发卡银行（403）与所述的账户安全服务器（5）相电讯连接，交易终端（3）通过有线/无线网络例如移动电话网络、WIFI 网络、区域网络、互联网络等等各类网络接入支付网络（4）的收单银行（402），发卡银行（403）于处理属于用户的银行卡账户的交易请求时，通过账户安全服务器（5）和该银行卡账户相关联的手机（2）进行验证该用户身份的安全验证。在第三实施例中，账户安全服务器（5）与发卡银行（403）相电讯连接，可以将账户安全服务器（5）

整合于发卡银行（403）中，所有属于发卡银行（403）的银行卡账户的交易支付都可以通过账户安全服务器（5）对用户的身份进行安全验证步骤，从而保障该银行的银行卡账户的安全。

继续参阅图 4，图 4 示出的第四实施例的支付网络（4）包括银行卡网络（401）、设有商户的银行账户的收单银行（402）、设有用户的银行卡账户的发卡银行（403）、支付网关（404），其中，银行卡网络（401）与发卡银行（403）相电讯连接，支付网关（404）分别与收单银行（402）和银行卡网络（401）相电讯连接，并与所述的账户安全服务器（5）相电讯连接，交易终端（3）通过有线/无线网络例如移动电话网络、WIFI 网络、区域网络、互联网络等等各类网络接入支付网络（4）的支付网关（404），支付网关（404）于处理属于用户的银行卡账户的交易请求时，通过账户安全服务器（5）和该银行卡账户相关联的手机（2）进行验证该用户身份的安全验证。在第四实施例中，支付网络（4）中包括了支付网关（404），这支付网关（404）是向商户的交易终端（3）和收单银行（402）提供网络服务，很多现有的信用卡支付系统都是采用这种架构。在本实施例中，账户安全服务器（5）与支付网关（404）相电讯连接，可以将账户安全服务器（5）整合于支付网关（404）中，所有通过支付网关（404）的处理的交易支付都可以通过账户安全服务器（5）对用户的身份进行安全验证步骤，从而保障用户的银行卡账户的安全。

以上已经详细说明本发明的第二至第四实施例，无论支付网络（4）采用第二实施例或第三实施例或第四实施例的方式来实现，都可以很好地实现本发明的目的，都是属于本发明的保护范围。

在本说明书中，所述的银行卡网络（401）包括 VISA 卡网络、中国银联卡网络、万事达卡网络、美国运通卡（American Express）网络、日本 JCB 卡网络、大来卡网络等等受理银行卡支付的网络，本发明都可以很好地应用于这些不同的支付网络。在本说明书中，所述的交易终端（3）是

指可以生成支付交易的设备，包括一般商户用于收款的 POS 机、可以受理信用卡的刷卡机、用于借记卡支付的刷卡机、用于非接触式金融卡的读卡机等等，也可以是一台计算机或服务器，例如购物网站的服务器，提供电话/电视购物服务的服务器，也可以是公共机构用于自动转账收费的账户服务器，也可以是银行 ATM 取款机，或网上银行服务中根据用户帐户操作生成交易的计算机等等，为了方便说明，在本说明书中一律称为交易终端（3）。此外，在本说明书中所述的银行卡（1）包括信用卡、借记卡、贷记卡、准贷记卡、转账卡、取款卡、提款卡等等之类由银行或金融机构发行用于支付或交易的卡，在本说明书中一律称为银行卡（1）。至于在本说明书中所述的手机（2），是指可以进行通讯的通讯工具，包括智能手机、平板电脑、个人数字助理（Personal Digital Assistant，简称 PDA）等等可以通过网络进行移动通讯的电子设备，为了方便说明，在本说明书中一律称为手机（2）。

本发明的主要特征，是在支付时通过账户安全服务器（5）与用户的手机（2）以实时通讯方式对用户的身份进行安全验证，账户安全服务器（5）可以根据风险高低或支付金额采用不同等级的安全验证，以下对不同等级的安全验证作进一步详细说明。

对于一些小金额支付，可以采用较简单等级的安全验证，例如账户安全服务器（5）核对用户的手机（2）是否已经成功接入账户安全服务器（5），如该手机（2）已经成功接入账户安全服务器（5）则安全验证成功，否则安全验证失败，只要用户的手机（2）处于开机状态，并且接入了账户安全服务器（5），用户就可以进行小金额支付。此外，也可以通过向用户的手机发送提示信息作为安全验证，所述的安全验证于支付时，由账户安全服务器（5）将有关交易的提示信息传送给用户的手机（2），如该提示信息已成功传送给该手机，则安全验证成功，否则安全验证失败。只要用户的手机（2）收到提示信息，就成功完成安全验证，用户可

以从提示信息中，知道自己的银行卡账户刚进行了一笔支付交易，如果用户并没有进行支付而收到提示信息，表示可能有人盗用用户的银行卡账户，用户就可以立即向银行报告或报警处理，减少损失。

除了上述简单等级的安全验证，对于一些大金额支付，可以采用较高等级的安全验证。要实现这较高等级的安全验证，须要预先为用户在账户安全服务器（5）设定一个用于确认的确认信息，这确认信息可以是一个密码，或是一个可动态改变的信息。在用户使用他的银行卡账户进行支付时，所述的安全验证除了由账户安全服务器（5）将有关交易的提示信息传送给用户的手机（2）外，还包括账户安全服务器（5）核对用户通过用户的手机（2）返回的确认信息；如账户安全服务器（5）核对该确认信息正确无误则安全验证成功，否则安全验证失败。即使用户的手机（2）和银行卡（1）同时被贼人盗取了，贼人没有正确的确认信息，是无法进行大金额支付，这样就保障了用户的银行卡账户安全。

对于一些大金额支付或风险较高的交易支付，还可以采用更进一步的安全验证，要求用户回答一些有关他个人信息的问题来验证用户的身份。要实现这样的安全验证，须要在所述的账户安全服务器（5）还储存有用用户的个人信息，例如用户的姓名、年龄、地址、电话号码、嗜好、职业、公司名称和地址等等，还可以包括用户的亲属的个人信息等等，也可以包括用户的最近交易记录等等，都可以作为用户的个人信息，账户安全服务器（5）进行安全验证时，随机选取用户的其中部分个人信息来生成一条或多条验证问题信息，然后将该验证问题信息传送给该用户的手机（2），用户要在指定时间内（例如 15 秒内）根据该验证问题信息向账户安全服务器（5）返回答案信息，账户安全服务器（5）核对返回的答案信息是否符合该验证问题信息的正确答案，如核对全部答案信息都符合验证问题信息的正确答案无误则安全验证成功，否则安全验证失败。例如，验证问题信息是“你的出生地是什么城市”，或者“你配偶的职业是什么”

等等与用户个人有关的问题，用户必须正确回答才能通过安全验证。此外，更可以将每一条验证问题配合一个正确答案和多个类似而错误的答案，以选择题方式让用户回答，方便用户更快返回答案信息。

以上所述的不同等级的安全验证，可以只选择其中之一单独用于本发明的系统和方法，也可以选择全部或部分应用于本发明的系统和方法，并根据支付金额或交易风险来决定安全验证的等级。例如小金额支付只须核对用户的手机（2）已接入账户安全服务器（5）；又例如用户在商店进行大金额支付时，须要用户通过手机（2）返回正确的确认信息；又例如用户进行网上支付，由于网上支付属于高风险类别，除了须要用户通过手机（2）返回正确的确认信息，还须要用户通过手机（2）回答多条验证问题，全部正确回答后才能通过安全验证。无论采用上述的那一个等级的安全验证，都可很好地实现本发明的目的，都是属于本发明的保护范围。

参阅图 5，图 5 是本发明第五实施例的银行卡安全支付系统的形像化示意说明图，图 5 示出了本发明应用于 ATM 取款机的实施例子。在第五实施例中，交易终端（3）是银行的 ATM 取款机，支付网络（4）就是设有用户银行卡账户的银行及其 ATM 网络，用户使用他的银行卡（1）在 ATM 取款机进行交易时，例如取款、转账等属于从用户的银行卡账户支出款项的交易，支付网络（4）立即通过账户安全服务器（5）和该银行卡账户的相关联的手机（2）进行验证该用户身份的安全验证，安全验证成功后用户才能成功进行该交易，否则支付网络（4）拒绝该交易。

参阅图 6，图 6 是本发明第六实施例的银行卡安全支付系统的形像化示意说明图，图 6 示出了本发明应用于网上银行服务的实施例子。在第六实施例中，所述的交易终端（3）是网上银行服务器，用户使用可上网的计算机即上网终端（7）通过互联网络（6）接入网上银行服务器进行账户操作，例如转账、缴费、买股票等属于从用户的银行卡账户支出款项的交易，网上银行服务器根据用户的操作生成交易信息，并向支付网络（4）

发出交易请求，要求从用户的银行卡账户进行支付，支付网络（4）立即通过账户安全服务器（5）和该银行卡账户相关联的手机（2）进行验证该用户身份的安全验证，安全验证成功后支付网络（4）才进行该交易的支付，网上银行服务器才能完成该账户操作，否则支付网络（4）拒绝该交易的支付，令网上银行服务器不能完成该账户操作。本实施例与一般的网上银行系统相比，本实施例让用户通过手机（2）掌握自己的银行卡账户的安全，即使黑客盗取了用户的银行卡账户资料，黑客没有用户的手机（2）是无法成功通过网上银行盗用用户的银行卡账户。

参阅图 7，图 7 是本发明第七实施例的银行卡安全支付系统的形像化示意说明图，图 7 示出了本发明应用于网络购物的实施例子。在第七实施例中，所述的交易终端（3）是购物网站/网上商城/网上商店/软件网站/音乐网站/电影网站/等等通过网络进行销售货品/软件/服务/影音等等之类的网络商店的电子商务服务器，用户使用上网终端（7）通过互联网络（6）登入电子商务服务器即交易终端（3）下订单，电子商务服务器根据用户的订单生成交易信息，并向支付网络（4）发出交易请求，要求从用户的银行卡账户进行支付，支付网络（4）立即通过账户安全服务器（5）和该银行卡账户相关联的手机（2）进行验证用户身份的安全验证，安全验证成功后支付网络（4）才进行该订单交易的支付，否则支付网络（4）拒绝该订单交易的支付。此外，本实施例也同样适用于电视购物和电话购物等等的电子商户，用户下订单购物付款时，支付网络（4）立即通过账户安全服务器（5）和用户的手机（2）进行验证该用户身份的安全验证，安全验证成功后支付网络（4）才进行该订单交易的支付，否则支付网络（4）拒绝该订单交易的支付。

参阅图 8，图 8 是本发明第八实施例的银行卡安全支付系统的形像化示意说明图，图 8 示出了本发明应用于自动转账付费的实施例子。在第八实施例中，所述的交易终端（3）是自动转账账务系统，这自动转账账务

系统就是公共机构例如：电力公司、煤气公司、电话公司等等之类的公司的账务系统服务器，这些自动转账账务系统通常会定期通过银行从用户的银行账户转账交费。自动转账虽然方便快捷，但是很多自动转账账单并不是固定金额的，而是根据用量而定，用户一般在自动转账完成后收到月结单才知道转账金额，很多用户因担心会被多收费用而不敢使用自动转账，令自动转账难以广泛推行。在本实施例中，当自动转账账务系统即交易终端（3）向银行即支付网络（4）要求从用户的银行卡账户自动转账收取费用时，例如电力公司从用户的银行卡账户自动转账收取电费，支付网络（4）立即通过账户安全服务器（5）和该银行卡账户的相关联的手机（2）进行验证该用户身份的安全验证，安全验证成功后银行即支付网络（4）才进行该自动转账支付，否则支付网络（4）拒绝执行该自动转账支付。本实施例通过安全验证步骤让用户可以全权掌握自动转账的控制权，用户就不用担心会被多收费用，有利于自动转账的推广。

以上已经详细说明本发明的银行卡安全支付系统和方法，虽然本发明以上述的实施例加以说明，但是本发明并不仅限于此，在不离开本发明的精神和所附权利要求书的范围的情况下，可以作多种改变和变化。

本发明的利用实时通讯的银行卡安全支付系统和方法，可以保障用户的银行卡账户的安全。本发明的实施，会带来良好的效益，对银行和用户都十分裨益。

权利要求

1. 一种银行卡安全支付系统，其特征在于，所述的系统包括用户的银行卡账户和手机（2）、商户的交易终端（3）、支付网络（4）、账户安全服务器（5），其中，账户安全服务器（5）与支付网络（4）相电讯连接，账户安全服务器（5）设有实时通讯服务器端软件，用户的手机（2）设有实时通讯应用程序，手机（2）通过该实时通讯应用程序接入账户安全服务器（5），交易终端（3）接入支付网络（4），账户安全服务器（5）记录用户的银行卡账户的账户资料，用户的银行卡账户与该用户的手机（2）相关联，以及，当支付网络（4）收到商户的交易终端（3）传送来属于用户的银行卡账户的交易请求时，支付网络（4）通过账户安全服务器（5）和该银行卡账户相关联的手机（2）进行验证该用户身份的安全验证，安全验证成功后支付网络（4）才继续进行该交易的后续步骤，否则拒绝该交易。
2. 如权利要求 1 所述的银行卡安全支付系统，其特征在于，所述的支付网络（4）包括银行卡网络（401）、设有商户的银行账户的收单银行（402）、设有用户的银行卡账户的发卡银行（403），其中，银行卡网络（401）分别与收单银行（402）和发卡银行（403）相电讯连接，并与所述的账户安全服务器（5）相电讯连接，交易终端（3）接入支付网络（4）的收单银行（402），银行卡网络（401）于处理属于用户的银行卡账户的交易请求时，通过账户安全服务器（5）和该银行卡账户相关联的手机（2）进行验证该用户身份的安全验证。
3. 如权利要求 1 所述的银行卡安全支付系统，其特征在于，所述的支付网络（4）包括银行卡网络（401）、设有商户的银行账户的收单银行

(402)、设有用户的银行卡账户的发卡银行(403)，其中，银行卡网络(401)分别与收单银行(402)和发卡银行(403)相电讯连接，发卡银行(403)与所述的账户安全服务器(5)相电讯连接，交易终端(3)接入支付网络(4)的收单银行(402)，发卡银行(403)于处理属于用户的银行卡账户的交易请求时，通过账户安全服务器(5)和该银行卡账户相关联的手机(2)进行验证该用户身份的安全验证。

4. 如权利要求1所述的银行卡安全支付系统，其特征在于，所述的支付网络(4)包括银行卡网络(401)、设有商户的银行账户的收单银行(402)、设有用户的银行卡账户的发卡银行(403)、支付网关(404)，其中，银行卡网络(401)与发卡银行(403)相电讯连接，支付网关(404)分别与收单银行(402)和银行卡网络(401)相电讯连接，并与所述的账户安全服务器(5)相电讯连接，交易终端(3)接入支付网络(4)的支付网关(404)，支付网关(404)于处理属于用户的银行卡账户的交易请求时，通过账户安全服务器(5)和该银行卡账户相关联的手机(2)进行验证该用户身份的安全验证。
5. 如权利要求2至4任一项所述的银行卡安全支付系统，其特征在于，所述的银行卡网络(401)包括VISA卡网络、中国银联卡网络、万事达卡网络、美国运通卡网络、日本JCB卡网络、大来卡网络。
6. 如权利要求1至4任一项所述的银行卡安全支付系统，其特征在于，所述的交易终端(3)是银行的ATM取款机。

7. 如权利要求 1 至 4 任一项所述的银行卡安全支付系统，其特征在于，所述的交易终端（3）是网上银行服务器。
8. 如权利要求 1 至 4 任一项所述的银行卡安全支付系统，其特征在于，所述的交易终端（3）是网络商店的电子商务服务器。
9. 如权利要求 1 至 4 任一项所述的银行卡安全支付系统，其特征在于，所述的交易终端（3）是自动转账账务系统。
10. 一种银行卡安全支付方法，其特征在于，所述的方法包括设置账户安全服务器（5），在账户安全服务器（5）记录用户的银行卡账户的账户资料，并将用户的银行卡账户与该用户的手机（2）相关联，账户安全服务器（5）与支付网络（4）相电讯连接，账户安全服务器（5）设有实时通讯服务器端软件，用户的手机（2）设有实时通讯应用程序，手机（2）通过该实时通讯应用程序接入账户安全服务器（5），以及，当支付网络（4）收到商户的交易终端（3）传送来属于用户的银行卡账户的交易请求时，支付网络（4）通过账户安全服务器（5）和该银行卡账户的相关联的手机（2）进行验证该用户身份的安全验证，安全验证成功后支付网络（4）才继续进行该交易的后续步骤，否则拒绝该交易。
11. 如权利要求 10 所述的银行卡安全支付方法，其特征在于，所述的安全验证包括账户安全服务器（5）将有关所述交易的提示信息传送给用户的手机（2），如该提示信息已成功传送给该手机，则安全验证成功，否则安全验证失败。

12. 如权利要求 11 所述的银行卡安全支付方法，其特征在于，所述的安全验证还包括账户安全服务器（5）核对用户通过用户的手机（2）返回的确认信息；如账户安全服务器（5）核对该确认信息正确无误则安全验证成功，否则安全验证失败。

13. 如权利要求 10 至 12 任一项所述的银行卡安全支付方法，其特征在于，所述的账户安全服务器（5）储存有用户的个人信息，账户安全服务器（5）进行安全验证时，随机选取用户的其中部分个人信息来生成验证问题信息，然后将该验证问题信息传送给该用户的手机（2），用户要在指定时间内根据该验证问题信息向账户安全服务器（5）返回答案信息，账户安全服务器（5）核对返回的答案信息是否符合该验证问题信息的正确答案，如核对答案信息符合正确答案无误则安全验证成功，否则安全验证失败。

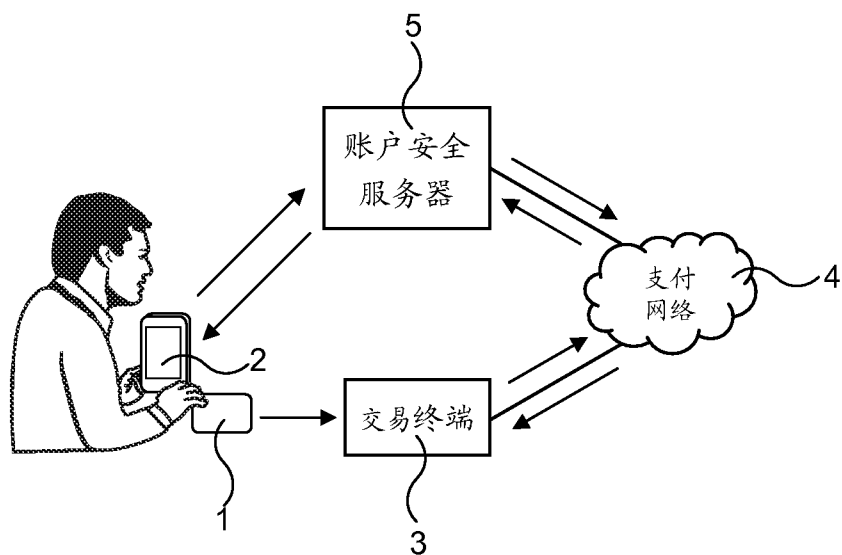


图 1

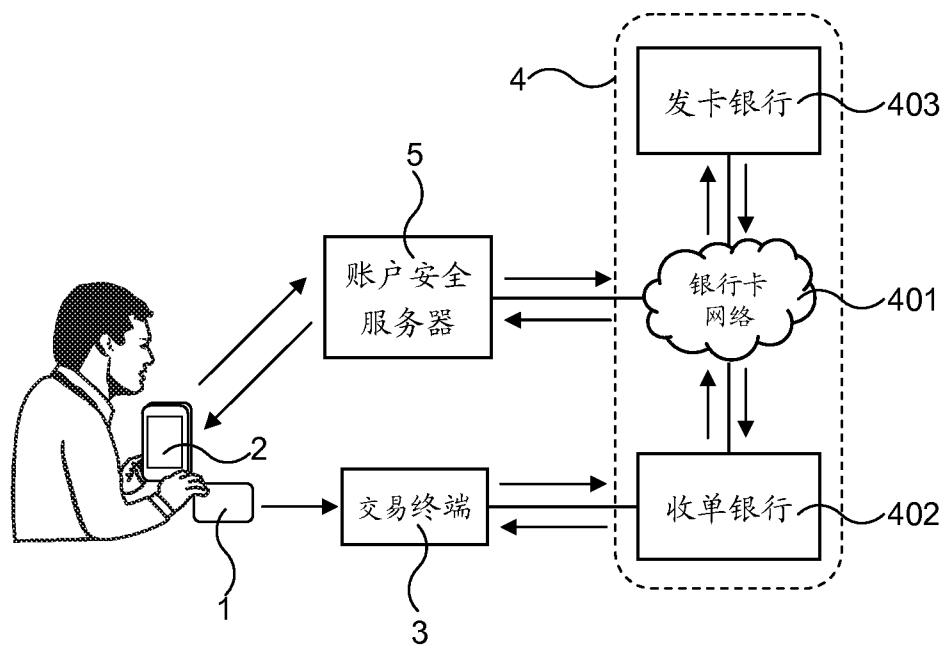


图 2

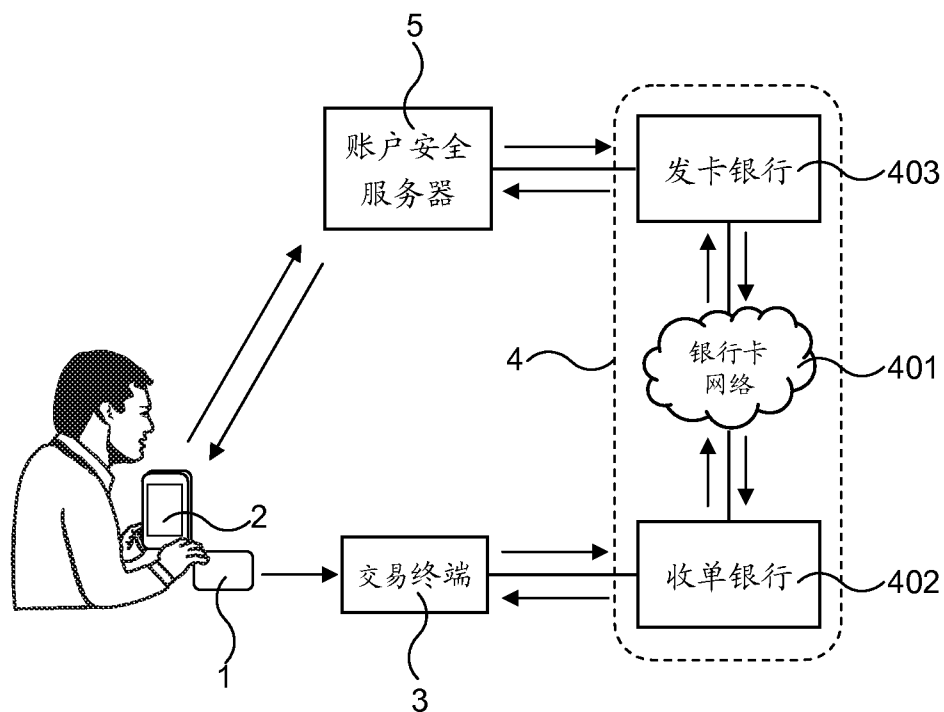


图 3

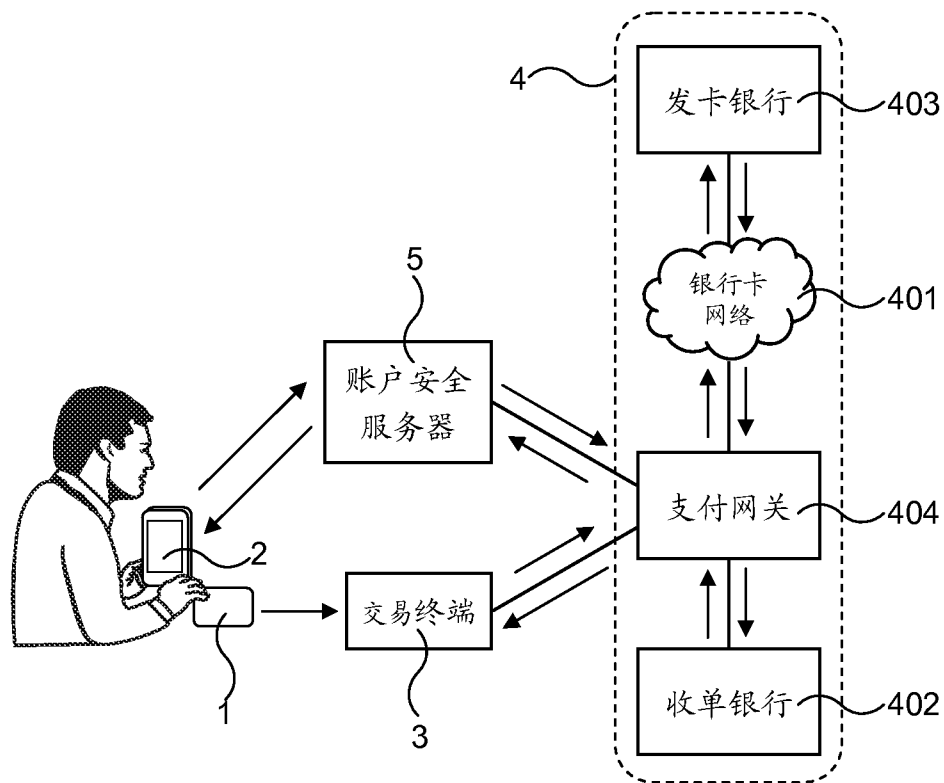


图 4

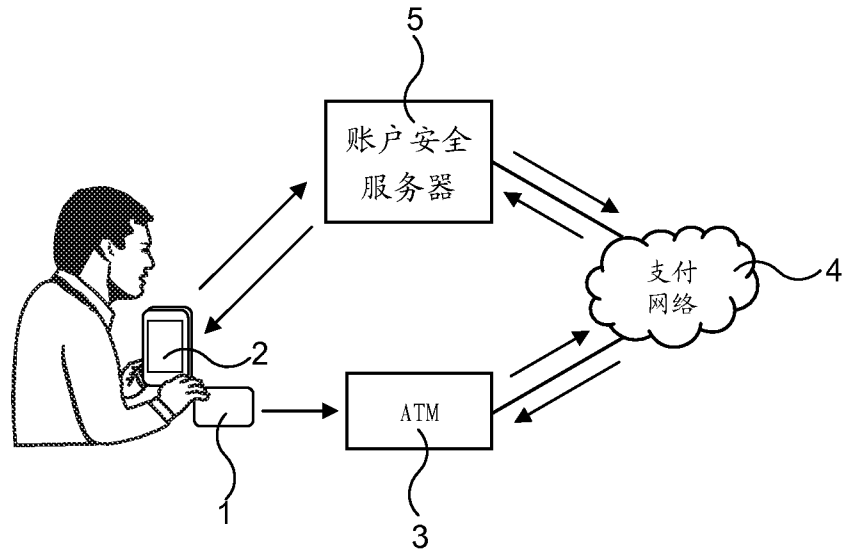


图 5

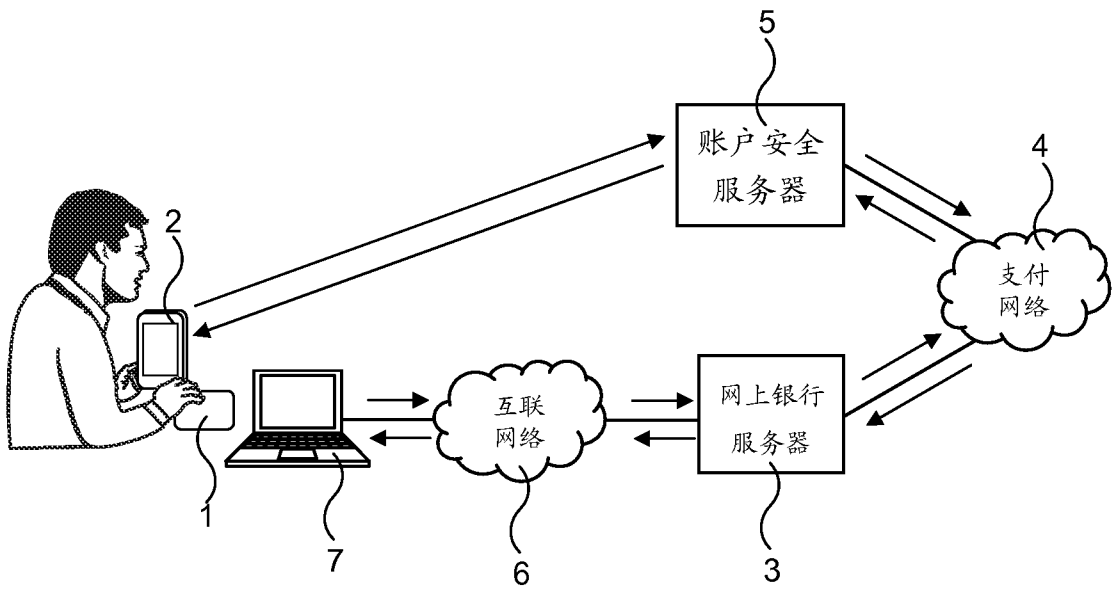


图 6

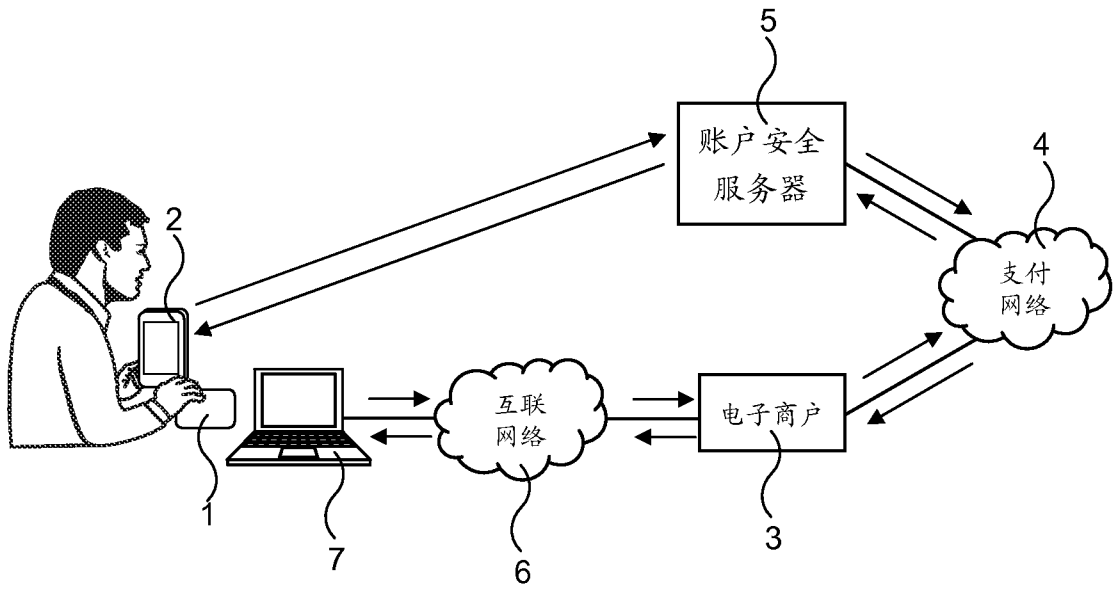


图 7

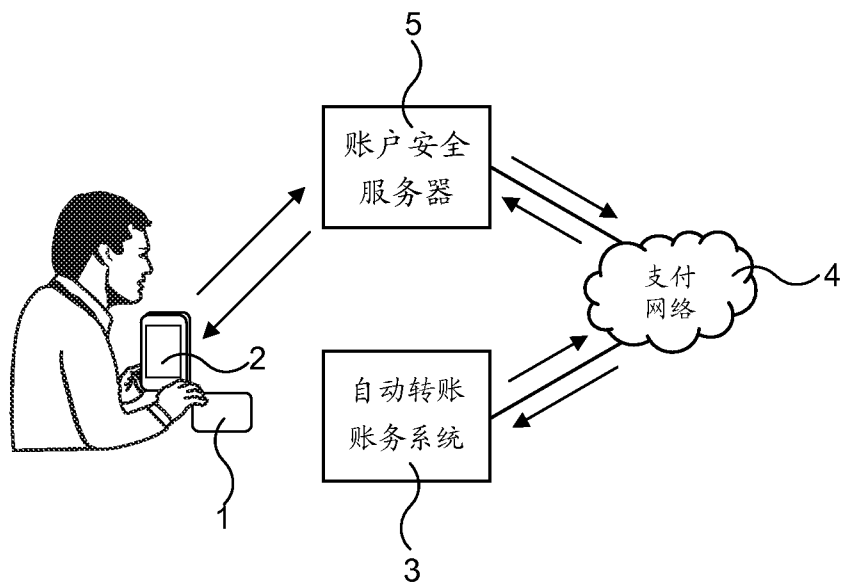


图 8

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2013/073030

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 102208069 A	05.10.2011	None	
CN 102542452 A	04.07.2012	None	
CN 101599192 A	09.12.2009	CN 101599192 B	18.05.2011
WO 0229742 A1	11.04.2002	AU 9395501 A	15.04.2002
		FR 2815203 A1	12.04.2002

A. 主题的分类 <p style="text-align: center;">G06Q 20/00 (2006.01) i</p> <p>按照国际专利分类(IPC)或者同时按照国家分类和 IPC 两种分类</p>																	
B. 检索领域 检索的最低限度文献(标明分类系统和分类号) <p style="text-align: center;">IPC: G06Q; H04L; H04W</p>																	
包含在检索领域中的除最低限度文献以外的检索文献 在国际检索时查阅的电子数据库(数据库的名称, 和使用的检索词 (如使用)) <p style="text-align: center;">CPRSABS, CNTXT, CNKI, VEN: 银行, 支付, 交易, 手机, 验证, 认证, 服务器, 终端, 银行卡, bank, payment, business, deal, handset, mobile w telephone, validat+, authenticat+, server, terminal, bank w card</p>																	
C. 相关文件																	
<table border="1" style="width:100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 10%;">类 型*</th> <th style="width: 70%;">引用文件, 必要时, 指明相关段落</th> <th style="width: 20%;">相关的权利要求</th> </tr> </thead> <tbody> <tr> <td style="text-align: center;">X</td> <td>CN102208069A (黄金富) 05. 10 月 2011 (05.10.2011) 参见说明书第 4-7 段, 附图 1</td> <td style="text-align: center;">1-13</td> </tr> <tr> <td style="text-align: center;">A</td> <td>CN102542452A (王筱雨) 04. 7 月 2012 (04.07.2012) 参见全文</td> <td style="text-align: center;">1-13</td> </tr> <tr> <td style="text-align: center;">A</td> <td>CN101599192A (北京华大智宝电子系统有限公司) 09. 12 月 2009 (09.12.2009) 参见全文</td> <td style="text-align: center;">1-13</td> </tr> <tr> <td style="text-align: center;">A</td> <td>WO0229742A1 (SOC NTSYS SA 等) 11. 4 月 2002 (11.04.2002) 参见全</td> <td style="text-align: center;">1-13</td> </tr> </tbody> </table>	类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求	X	CN102208069A (黄金富) 05. 10 月 2011 (05.10.2011) 参见说明书第 4-7 段, 附图 1	1-13	A	CN102542452A (王筱雨) 04. 7 月 2012 (04.07.2012) 参见全文	1-13	A	CN101599192A (北京华大智宝电子系统有限公司) 09. 12 月 2009 (09.12.2009) 参见全文	1-13	A	WO0229742A1 (SOC NTSYS SA 等) 11. 4 月 2002 (11.04.2002) 参见全	1-13	<input type="checkbox"/> 其余文件在 C 栏的续页中列出。 <input checked="" type="checkbox"/> 见同族专利附件。	
类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求															
X	CN102208069A (黄金富) 05. 10 月 2011 (05.10.2011) 参见说明书第 4-7 段, 附图 1	1-13															
A	CN102542452A (王筱雨) 04. 7 月 2012 (04.07.2012) 参见全文	1-13															
A	CN101599192A (北京华大智宝电子系统有限公司) 09. 12 月 2009 (09.12.2009) 参见全文	1-13															
A	WO0229742A1 (SOC NTSYS SA 等) 11. 4 月 2002 (11.04.2002) 参见全	1-13															
* 引用文件的具体类型: “A” 认为不特别相关的表示了现有技术一般状态的文件 “E” 在国际申请日的当天或之后公布的在先申请或专利 “L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件 (如具体说明的) “O” 涉及口头公开、使用、展览或其他方式公开的文件 “P” 公布日先于国际申请日但迟于所要求的优先权日的文件	“T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件 “X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性 “Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性 “&” 同族专利的文件																
国际检索实际完成的日期 <p style="text-align: center;">28. 11 月 2013 (28.11.2013)</p>	国际检索报告邮寄日期 <p style="text-align: center;">26.12 月 2013 (26.12.2013)</p>																
ISA/CN 的名称和邮寄地址: 中华人民共和国国家知识产权局 中国北京市海淀区蓟门桥西土城路 6 号 100088 传真号: (86-10)62019451	受权官员 <p style="text-align: center;">元晓旭</p> 电话号码: (86-10) 62412030																

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2013/073030

检索报告中引用的 专利文件	公布日期	同族专利	公布日期
CN102208069A	05.10.2011	无	
CN102542452A	04.07.2012	无	
CN101599192A	09.12.2009	CN101599192B	18.05.2011
WO0229742A1	11.04.2002	AU9395501A	15.04.2002
		FR2815203A1	12.04.2002