(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 4 月 3 日 (03.04.2014)

WIPO | PCT

(10) 国际公布号
WO 2014/048319 A1

(51) 国际专利分类号:
H04L 29/06 (2006.01)

(21) 国际申请号: PCT/CN2013/084183

(22) 国际申请日: 2013 年 9 月 25 日 (25.09.2013)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201210368401.3 2012 年 9 月 28 日 (28.09.2012) CN

(71) 申请人: **中国银联股份有限公司 (CHINA UNIONPAY CO., LTD.)** [CN/CN]; 中国上海市浦东新区含笑路 36 号银联大厦, Shanghai 200135 (CN)。

(72) 发明人: **柴洪峰 (CHAI, Hongfeng)**; 中国上海市浦东新区含笑路 36 号银联大厦 7 楼, Shanghai 200135 (CN)。 **鲁志军 (LU, Zhijun)**; 中国上海市浦东新区含笑路 36 号银联大厦 7 楼, Shanghai 200135 (CN)。 **何朔 (HE, Shuo)**; 中国上海市浦东新区含笑路 36 号银联大厦 7 楼, Shanghai 200135 (CN)。 **郑建宾 (ZHENG, Jianbin)**; 中国上海市浦东新区含笑路 36 号银联大厦 7 楼, Shanghai 200135 (CN)。 **刘国宝 (LIU, Guobao)**; 中国上海市浦东新区含笑路 36 号银联大厦 7 楼, Shanghai 200135 (CN)。 **万四爽 (WAN, Sishuang)**; 中国上海市浦东新区含笑路 36 号银联大厦 7 楼, Shanghai 200135 (CN)。

(74) 代理人: **中国专利代理（香港）有限公司 (CHINA PATENT AGENT (HK) 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, 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,

[见续页]

(54) Title: SECURITY INFORMATION EXCHANGE SYSTEM, APPARATUS, AND METHOD

(54) 发明名称 : 安全性信息交互系统、设备及方法

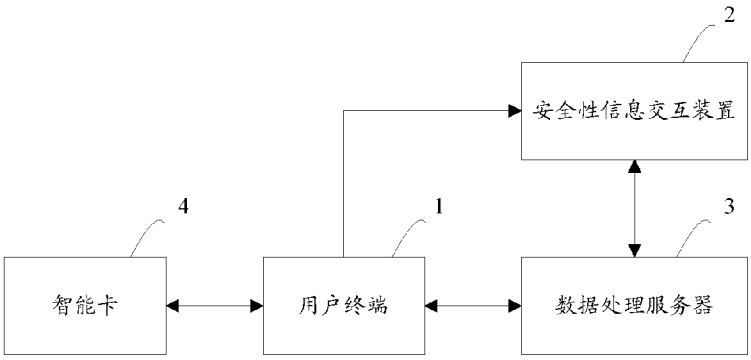


图 1 /Fig.1

1 User terminal
2 Security information exchange device
3 Data processing server
4 Smart card

(57) Abstract: A security information exchange system, apparatus and method are provided. The system comprises at least one user terminal, a security information exchange device, a data processing server, and a smart card. Each user-originated security information exchange command in the at least one user terminal is transmitted via a network to a remote security information exchange device for further security information exchange processing. The disclosed security information exchange system, device and method are highly secure and can be used for offline remote information exchange.

(57) 摘要: 本发明提出了安全性信息交互系统、设备及方法。其中，所述系统包括至少一个用户终端、安全性信息交互装置，数据处理服务器和智能卡，所述至少一个用户终端中的每个将来自用户的安全性信息交互指令通过网络传送到远程安全性信息交互装置以完成后续的安全性信息交互过程。本发明所公开的安全性信息交互系统、设备及方法具有高的安全性并且能够应用于脱机方式的远程信息交互。

WO 2014/048319 A1

RO, RS, RU, RW, SA, 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, KM, 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))。

安全性信息交互系统、设备及方法

技术领域

本发明涉及信息交互系统、设备及方法，更具体地，涉及安全性信息交互系统、设备及方法。

背景技术

目前，随着网络应用的日益广泛以及不同领域的业务种类的日益丰富，通过网络（特别是移动网络）进行脱机方式的安全性信息（即对安全性要求较高的信息，例如与金融交易相关的信息）的交互变得越来越重要。

现有的脱机方式的安全性信息交互系统及方法通常应用于现场形式的信息交互（例如电子现金的现场脱机支付）。因此，其存在如下问题：难于在远程的信息交互（例如电子现金的远程脱机支付）中应用（例如由于用户的移动终端通常是不可信的，故造成现有的信息交互机制和安全机制不适用于基于移动网络的远程信息交互）。

因此，存在如下需求：提供具有高的安全性并且能够应用于脱机方式的远程信息交互的安全性信息交互系统、设备及方法。

发明内容

为了解决上述现有技术方案中所存在的问题，本发明提出了具有高的安全性并且能够应用于脱机方式的远程信息交互的安全性信息交互系统、设备及方法。

本发明的目的是通过以下技术方案实现的：

一种安全性信息交互方法，所述安全性信息交互方法包括下列步骤：

（A1）用户终端将来自用户的安全性信息交互指令通过网络传送到远程安全性信息交互装置；

（A2）所述安全性信息交互装置接收来自所述用户终端的所述安全性信息交互指令，并基于所述安全性信息交互指令构造安全性信息交互

请求以及将所述安全性信息交互请求传送到数据处理服务器;

（A3）所述数据处理服务器接收并解析来自所述安全性信息交互装置的所述安全性信息交互请求，并基于所述安全性信息交互请求向所述用户终端发送安全性信息交互确认请求;

（A4）所述用户终端接收来自所述数据处理服务器的所述安全性信息交互确认请求，以及基于所述安全性信息交互确认请求从智能卡中的脱机应用获取应用数据并将所述应用数据传送到所述数据处理服务器;

（A5）所述数据处理服务器接收所述用户终端传送回的所述应用数据，并基于所述应用数据执行认证操作以及将认证结果通知传送回所述用户终端;

（A6）所述用户终端接收来自所述数据处理服务器的认证结果通知，并基于所述认证结果通知生成安全性信息交互数据以及将所述安全性信息交互数据传送到所述数据处理服务器;

（A7）所述数据处理服务器接收来自所述用户终端的所述安全性信息交互数据，并基于所述安全性信息交互数据执行验证操作以及将与验证结果相关的消息传送到所述安全性信息交互装置。

在上面所公开的方案中，优选地，所述步骤（A7）进一步包括：如果所述验证结果是“验证成功”，则所述数据处理服务器向所述用户终端发送安全性信息交互成功应答。

在上面所公开的方案中，优选地，所述步骤（A7）进一步包括：如果所述验证结果是“验证成功”，则所述数据处理服务器将与验证结果相关的通知发送到业务提供方服务器。

在上面所公开的方案中，优选地，所述用户终端是移动终端中的客户端，并且所述网络是移动通信网络。

在上面所公开的方案中，优选地，所述应用数据包括脱机认证数据和用于终端风险管理和行为分析的数据。

在上面所公开的方案中，优选地，所述步骤（A5）进一步包括：在接收到所述用户终端传送回的所述应用数据后，所述数据处理服务器执行如下操作：解析所述应用数据以获得脱机认证数据和用于终端风险管

理和行为分析的数据；基于所述脱机认证数据执行认证操作，并且如果认证结果为“认证未通过”，则向所述用户终端传送回安全性信息交互拒绝应答；如果认证结果为“认证通过”，则执行终端风险管理和行为分析操作以确定是否进行后续的安全性信息交互过程，并且如果确定进行后续的安全性信息交互过程，则向所述用户终端传送回安全性信息交互批准应答，以及如果确定不需进行后续的安全性信息交互过程，则向所述用户终端传送回安全性信息交互拒绝应答。

在上面所公开的方案中，优选地，所述步骤（A6）进一步包括：在接收到来自所述数据处理服务器的认证结果通知后，所述用户终端执行如下操作：如果所述认证结果通知是安全性信息交互拒绝应答，则提示用户安全性信息交互失败，并且如果所述认证结果通知是安全性信息交互批准应答，则执行与当前进行的安全性信息交互过程相关联的数据处理操作并生成所述安全性信息交互数据，以及将所述安全性信息交互数据传送到所述数据处理服务器。

在上面所公开的方案中，优选地，所述安全性信息交互数据包括安全性信息交互凭证和其他与当前进行的安全性信息交互过程相关联的信息。

在上面所公开的方案中，优选地，所述步骤（A7）进一步包括：所述数据处理服务器验证所述安全性信息交互凭证。

在上面所公开的方案中，优选地，通过 SSL 协议实现所述安全性信息交互装置与所述数据处理服务器之间的数据通信。

在上面所公开的方案中，优选地，通过 SSL 协议实现所述用户终端与所述数据处理服务器之间的数据通信。

在上面所公开的方案中，优选地，所述步骤（A6）进一步包括：以加密的方式传送所述安全性信息交互数据，其中，将安全性信息交互标识符作为加密密钥的生成因子。

在上面所公开的方案中，优选地，所述步骤（A4）进一步包括：所述用户终端以如下方式从脱机应用获取所述应用数据：（1）向所述智能卡发送选择脱机应用的指令以选择脱机应用；（2）初始化所述脱机应用；

（3）提示用户输入针对所述脱机应用的PIN从而验证用户的身份，并且如果验证通过，则执行后续操作，而如果验证未通过，则提示重新输入所述针对所述脱机应用的PIN，并重复验证过程，以及如果输入次数超过预定的阈值则提示用户身份验证失败；向所述脱机应用发送读取应用数据指令以获取所述应用数据。

本发明的目的还可以通过以下技术方案实现：

一种安全性信息交互系统，所述安全性信息交互系统包括：

至少一个用户终端，所述至少一个用户终端中的每个用于将来自用户的安全性信息交互指令通过网络传送到远程安全性信息交互装置，并接收来自数据处理服务器的安全性信息交互确认请求，以及基于所述安全性信息交互确认请求从脱机应用获取应用数据并将所述应用数据传送到所述数据处理服务器，所述至少一个用户终端中的每个进一步用于接收来自所述数据处理服务器的认证结果通知，并基于所述认证结果通知生成安全性信息交互数据以及将所述安全性信息交互数据传送到所述数据处理服务器；

安全性信息交互装置，所述安全性信息交互装置用于接收来自所述用户终端的所述安全性信息交互指令，并基于所述安全性信息交互指令构造安全性信息交互请求以及将所述安全性信息交互请求传送到所述数据处理服务器；

数据处理服务器，所述数据处理服务器用于接收并解析来自所述安全性信息交互装置的所述安全性信息交互请求，并基于所述安全性信息交互请求向相应的用户终端发送所述安全性信息交互确认请求，所述数据处理服务器进一步用于接收所述用户终端传送回的应用数据，并基于所述应用数据执行认证操作以及将认证结果通知传送回相应的用户终端，所述数据处理服务器进一步用于接收来自所述用户终端的所述安全性信息交互数据，并基于所述安全性信息交互数据执行验证操作以及将与验证结果相关的消息传送到所述安全性信息交互装置；

智能卡，所述智能卡用于存储至少一个脱机应用。

本发明的目的还可以通过以下技术方案实现：

一种用户终端，所述用户终端将来自用户的安全性信息交互指令通过网络传送到远程安全性信息交互装置，并接收来自数据处理服务器的安全性信息交互确认请求，以及基于所述安全性信息交互确认请求从智能卡中的脱机应用获取应用数据并将所述应用数据传送到所述数据处理服务器，所述用户终端进一步用于接收来自所述数据处理服务器的认证结果通知，并基于所述认证结果通知生成安全性信息交互数据以及将所述安全性信息交互数据传送到所述数据处理服务器。

本发明的目的还可以通过以下技术方案实现:

一种数据处理服务器，所述数据处理服务器接收并解析来自安全性信息交互装置的安全性信息交互请求，并基于所述安全性信息交互请求向相应的用户终端发送安全性信息交互确认请求，所述数据处理服务器进一步用于接收所述用户终端传送回的应用数据，并基于所述应用数据执行认证操作以及将认证结果通知传送回相应的用户终端，所述数据处理服务器进一步用于接收来自所述用户终端的安全性信息交互数据，并基于所述安全性信息交互数据执行验证操作以及将与验证结果相关的消息传送到所述安全性信息交互装置。

本发明所公开的安全性信息交互系统、设备及方法具有如下优点:（1）能够应用于脱机方式的远程信息交互;（2）由于使用了多种安全措施（例如，以加密的方式传送安全性信息交互数据，其中，将安全性信息交互标识符（诸如订单号）作为加密密钥的生成因子），故具有高的安全性。

附图说明

结合附图，本发明的技术特征以及优点将会被本领域技术人员更好地理解，其中:

图1是根据本发明的实施例的安全性信息交互系统的示意性结构图;

图2是根据本发明的实施例的安全性信息交互方法的流程图。

具体实施方式

图1是根据本发明的实施例的安全性信息交互系统的示意性结构图。如图1所示，本发明所公开的安全性信息交互系统包括至少一个用户终端1、安全性信息交互装置2（例如POS机），数据处理服务器3和智能卡4。其中，所述至少一个用户终端1中的每个用于将来自用户的安全性信息交互指令（例如购买请求）通过网络传送到远程安全性信息交互装置2，并接收来自数据处理服务器3的安全性信息交互确认请求（例如订单支付请求），以及基于所述安全性信息交互确认请求从脱机应用获取应用数据并将所述应用数据传送到所述数据处理服务器3，所述至少一个用户终端1中的每个进一步用于接收来自所述数据处理服务器3的认证结果通知，并基于所述认证结果通知生成安全性信息交互数据以及将所述安全性信息交互数据传送到所述数据处理服务器3。所述安全性信息交互装置2用于接收来自所述用户终端1的所述安全性信息交互指令，并基于所述安全性信息交互指令构造安全性信息交互请求（例如订单）以及将所述安全性信息交互请求传送到所述数据处理服务器3。所述数据处理服务器3用于接收并解析来自所述安全性信息交互装置2的所述安全性信息交互请求，并基于所述安全性信息交互请求向相应的用户终端1发送所述安全性信息交互确认请求，所述数据处理服务器3进一步用于接收所述用户终端1传送回的应用数据，并基于所述应用数据执行认证操作以及将认证结果通知传送回相应的用户终端1，所述数据处理服务器3进一步用于接收来自所述用户终端1的所述安全性信息交互数据，并基于所述安全性信息交互数据执行验证操作以及将与验证结果相关的消息（例如支付成功确认通知）传送到所述安全性信息交互装置2（例如用于提醒商户开始发货）。所述智能卡4用于存储至少一个脱机应用。

优选地，在本发明所公开的安全性信息交互系统中，所述数据处理服务器3进一步用于执行如下操作：如果所述验证结果是“验证成功”，则向相应的用户终端1发送安全性信息交互成功应答（例如支付成功应答，用于提示用户已经支付完成）。

优选地，在本发明所公开的安全性信息交互系统中，所述数据处理服务器3进一步用于执行如下操作：如果所述验证结果是“验证成功”，

则将与验证结果相关的通知（例如支付结果通知）发送到业务提供方服务器（例如发卡行的相关服务器）。

优选地，在本发明所公开的安全性信息交互系统中，所述用户终端1是移动终端中的客户端，并且所述网络是移动通信网络。

优选地，在本发明所公开的安全性信息交互系统中，所述应用数据包括脱机认证数据和用于终端风险管理和行为分析的数据。

优选地，在本发明所公开的安全性信息交互系统中，在接收到所述用户终端1传送回的所述应用数据后，所述数据处理服务器3执行如下操作：解析所述应用数据以获得脱机认证数据和用于终端风险管理和行为分析的数据；基于所述脱机认证数据执行认证操作，并且如果认证结果为“认证未通过”，则向相应的用户终端1传送回安全性信息交互拒绝应答；如果认证结果为“认证通过”，则执行终端风险管理和行为分析操作（例如判断电子现金可用余额减去授权金额是否小于电子现金重置阈值）以确定是否进行后续的安全性信息交互过程，并且如果确定进行后续的安全性信息交互过程，则向相应的用户终端1传送回安全性信息交互批准应答，以及如果确定不需进行后续的安全性信息交互过程，则向相应的用户终端1传送回安全性信息交互拒绝应答。

优选地，在本发明所公开的安全性信息交互系统中，在接收到来自所述数据处理服务器3的认证结果通知后，所述用户终端1执行如下操作：如果所述认证结果通知是安全性信息交互拒绝应答，则提示用户安全性信息交互失败，并且如果所述认证结果通知是安全性信息交互批准应答，则执行与当前进行的安全性信息交互过程相关联的数据处理操作（例如对电子现金进行扣款）并生成所述安全性信息交互数据，以及将所述安全性信息交互数据传送到所述数据处理服务器3。

优选地，在本发明所公开的安全性信息交互系统中，所述安全性信息交互数据包括安全性信息交互凭证（例如交易扣款凭证）和其他与当前进行的安全性信息交互过程相关联的信息（例如安全性信息交互标识符，诸如订单号）。

优选地，在本发明所公开的安全性信息交互系统中，所述数据处理

服务器3执行的所述验证操作包括验证所述安全性信息交互凭证。

优选地，在本发明所公开的安全性信息交互系统中，所述安全性信息交互装置2是所述网络中的节点（即可以通过所述网络与外部设备进行数据通信）。

优选地，在本发明所公开的安全性信息交互系统中，通过 SSL 协议实现所述安全性信息交互装置2与所述数据处理服务器3之间的数据通信。

优选地，在本发明所公开的安全性信息交互系统中，通过 SSL 协议实现所述用户终端1与所述数据处理服务器3之间的数据通信。

优选地，在本发明所公开的安全性信息交互系统中，通过对称密钥体系实现所述认证过程。

优选地，在本发明所公开的安全性信息交互系统中，以加密的方式传送所述安全性信息交互数据（其包括安全性信息交互凭证），其中，将安全性信息交互标识符（诸如订单号）作为加密密钥的生成因子。

示例性地，在本发明所公开的安全性信息交互系统中，所述智能卡4可以是 SIM 卡，或智能 SD 卡，或终端附件等。

优选地，在本发明所公开的安全性信息交互系统中，所述用户终端1以如下方式从脱机应用获取所述应用数据：（1）向所述智能卡4发送选择脱机应用的指令以选择脱机应用；（2）初始化所述脱机应用；（3）提示用户输入针对所述脱机应用的 PIN（个人识别码）从而验证用户的身份，并且如果验证通过，则执行后续操作，而如果验证未通过，则提示重新输入所述针对所述脱机应用的 PIN，并重复验证过程，以及如果输入次数超过预定的阈值则提示用户身份验证失败；向所述脱机应用发送读取应用数据指令以获取所述应用数据。

示例性地，在金融领域中，所述与当前进行的安全性信息交互过程相关联的数据处理操作可以是为了完成交易而对电子现金进行的扣款操作，并且具体的操作过程可以如下：所述用户终端 1 向所述智能卡 4 发送扣款请求；收到扣款请求后，所述智能卡 4 执行卡片风险分析以决定是否批准该交易请求；如果批准，则返回脱机交易批准密文 TC，此时卡

内的电子现金金额已经进行了更新；如果不批准，则返回拒绝响应（例如密文 AAC）；用户终端 1 判断是否为脱机交易批准 TC 密文，并且如果是，则组装脱机交易扣款凭证，并将该凭证发送给所述智能卡 4 进行加密和 MAC 计算；所述智能卡 4 确认该脱机交易扣款凭证确实属于本帐户的有效脱机交易数据（即未经处理过的属于本帐户的脱机交易数据），则完成相关的安全操作，而如果确认不是，则返回错误指示。

由上可见，本发明所公开的安全性信息交互系统具有如下优点：（1）能够应用于脱机方式的远程信息交互；（2）由于使用了多种安全措施（例如，以加密的方式传送安全性信息交互数据，其中，将安全性信息交互标识符（诸如订单号）作为加密密钥的生成因子），故具有高的安全性。

如图1所示，本发明公开了一种用户终端1，所述用户终端1将来自用户的安全性信息交互指令（例如购买请求）通过网络传送到远程安全性信息交互装置2，并接收来自数据处理服务器3的安全性信息交互确认请求（例如订单支付请求），以及基于所述安全性信息交互确认请求从智能卡4中的脱机应用获取应用数据并将所述应用数据传送到所述数据处理服务器3，所述用户终端1进一步用于接收来自所述数据处理服务器3的认证结果通知，并基于所述认证结果通知生成安全性信息交互数据以及将所述安全性信息交互数据传送到所述数据处理服务器3。

优选地，本发明所公开的用户终端1是移动终端中的客户端，并且所述网络是移动通信网络。

优选地，在本发明所公开的用户终端1中，所述应用数据包括脱机认证数据和用于终端风险管理和行为分析的数据。

优选地，在接收到来自所述数据处理服务器3的认证结果通知后，所述用户终端1执行如下操作：如果所述认证结果通知是安全性信息交互拒绝应答，则提示用户安全性信息交互失败，并且如果所述认证结果通知是安全性信息交互批准应答，则执行与当前进行的安全性信息交互过程相关联的数据处理操作（例如对电子现金进行扣款）并生成所述安全性信息交互数据，以及将所述安全性信息交互数据传送到所述数据处理服务器3。

优选地，在本发明所公开的用户终端1中，所述安全性信息交互数据包括安全性信息交互凭证（例如交易扣款凭证）和其他与当前进行的安全性信息交互过程相关联的信息（例如安全性信息交互标识符，诸如订单号）。

优选地，本发明所公开的用户终端1通过SSL协议与所述数据处理服务器3进行数据通信。

优选地，本发明所公开的用户终端1以加密的方式传送所述安全性信息交互数据（其包括安全性信息交互凭证），其中，将安全性信息交互标识符（诸如订单号）作为加密密钥的生成因子。

优选地，本发明所公开的用户终端1以如下方式从脱机应用获取所述应用数据:（1）向所述智能卡4发送选择脱机应用的指令以选择脱机应用;（2）初始化所述脱机应用;（3）提示用户输入针对所述脱机应用的PIN（个人识别码）从而验证用户的身份，并且如果验证通过，则执行后续操作，而如果验证未通过，则提示重新输入所述针对所述脱机应用的PIN，并重复验证过程，以及如果输入次数超过预定的阈值则提示用户身份验证失败；向所述脱机应用发送读取应用数据指令以获取所述应用数据。

如图1所示，本发明公开了一种数据处理服务器3，所述数据处理服务器3接收并解析来自安全性信息交互装置2的安全性信息交互请求，并基于所述安全性信息交互请求向相应的用户终端1发送安全性信息交互确认请求，所述数据处理服务器3进一步用于接收所述用户终端1传送回的应用数据，并基于所述应用数据执行认证操作以及将认证结果通知传送回相应的用户终端1，所述数据处理服务器3进一步用于接收来自所述用户终端1的安全性信息交互数据，并基于所述安全性信息交互数据执行验证操作以及将与验证结果相关的消息（例如支付成功确认通知）传送到所述安全性信息交互装置2（例如用于提醒商户开始发货）。

优选地，本发明所公开的数据处理服务器3进一步用于执行如下操作：如果所述验证结果是“验证成功”，则向相应的用户终端1发送安全性信息交互成功应答（例如支付成功应答，用于提示用户已经支付完成）。

优选地，本发明所公开的数据处理服务器3进一步用于执行如下操

作：如果所述验证结果是“验证成功”，则将与验证结果相关的通知（例如支付结果通知）发送到业务提供方服务器（例如发卡行的相关服务器）。

优选地，在本发明所公开的数据处理服务器3中，所述应用数据包括脱机认证数据和用于终端风险管理和行为分析的数据。

优选地，在接收到所述用户终端1传送回的所述应用数据后，所述数据处理服务器3执行如下操作：解析所述应用数据以获得脱机认证数据和用于终端风险管理和行为分析的数据；基于所述脱机认证数据执行认证操作，并且如果认证结果为“认证未通过”，则向相应的用户终端1传送回安全性信息交互拒绝应答；如果认证结果为“认证通过”，则执行终端风险管理和行为分析操作（例如判断电子现金可用余额减去授权金额是否小于电子现金重置阈值）以确定是否进行后续的安全性信息交互过程，并且如果确定进行后续的安全性信息交互过程，则向相应的用户终端1传送回安全性信息交互批准应答，以及如果确定不需进行后续的安全性信息交互过程，则向相应的用户终端1传送回安全性信息交互拒绝应答。

优选地，在本发明所公开的数据处理服务器3中，所述安全性信息交互数据包括安全性信息交互凭证（例如交易扣款凭证）和其他与当前进行的安全性信息交互过程相关联的信息（例如安全性信息交互标识符，诸如订单号）。

优选地，本发明所公开的数据处理服务器3执行的所述验证操作包括验证所述安全性信息交互凭证。

优选地，本发明所公开的数据处理服务器3通过 SSL 协议与所述安全性信息交互装置2进行数据通信。

优选地，本发明所公开的数据处理服务器3通过 SSL 协议与所述用户终端1进行数据通信。

优选地，在本发明所公开的数据处理服务器3中，通过对称密钥体系实现所述认证过程。

图2是根据本发明的实施例的安全性信息交互方法的流程图。如图2所示，本发明所公开的安全性信息交互方法包括下列步骤：（A1）用户终端将来自用户的安全性信息交互指令（例如购买请求）通过网络传送到

远程安全性信息交互装置；（A2）所述安全性信息交互装置接收来自所述用户终端的所述安全性信息交互指令，并基于所述安全性信息交互指令构造安全性信息交互请求（例如订单）以及将所述安全性信息交互请求传送到数据处理服务器；（A3）所述数据处理服务器接收并解析来自所述安全性信息交互装置的所述安全性信息交互请求，并基于所述安全性信息交互请求向所述用户终端发送安全性信息交互确认请求；（A4）所述用户终端接收来自所述数据处理服务器的所述安全性信息交互确认请求（例如订单支付请求），以及基于所述安全性信息交互确认请求从智能卡中的脱机应用获取应用数据并将所述应用数据传送到所述数据处理服务器；（A5）所述数据处理服务器接收所述用户终端传送回的所述应用数据，并基于所述应用数据执行认证操作以及将认证结果通知传送回所述用户终端；（A6）所述用户终端接收来自所述数据处理服务器的认证结果通知，并基于所述认证结果通知生成安全性信息交互数据以及将所述安全性信息交互数据传送到所述数据处理服务器；（A7）所述数据处理服务器接收来自所述用户终端的所述安全性信息交互数据，并基于所述安全性信息交互数据执行验证操作以及将与验证结果相关的消息（例如支付成功确认通知）传送到所述安全性信息交互装置（例如用于提醒商户开始发货）。

优选地，在本发明所公开的安全性信息交互方法中，所述步骤（A7）进一步包括：如果所述验证结果是“验证成功”，则所述数据处理服务器向所述用户终端发送安全性信息交互成功应答（例如支付成功应答，用于提示用户已经支付完成）。

优选地，在本发明所公开的安全性信息交互方法中，所述步骤（A7）进一步包括：如果所述验证结果是“验证成功”，则所述数据处理服务器将与验证结果相关的通知（例如支付结果通知）发送到业务提供方服务器（例如发卡行的相关服务器）。

优选地，在本发明所公开的安全性信息交互方法中，所述用户终端是移动终端中的客户端，并且所述网络是移动通信网络。

优选地，在本发明所公开的安全性信息交互方法中，所述应用数据包括脱机认证数据和用于终端风险管理和行为分析的数据。

优选地，在本发明所公开的安全性信息交互方法中，所述步骤（A5）进一步包括：在接收到所述用户终端传送回的所述应用数据后，所述数据处理服务器执行如下操作：解析所述应用数据以获得脱机认证数据和用于终端风险管理和行为分析的数据；基于所述脱机认证数据执行认证操作，并且如果认证结果为“认证未通过”，则向所述用户终端传送回安全性信息交互拒绝应答；如果认证结果为“认证通过”，则执行终端风险管理和行为分析操作（例如判断电子现金可用余额减去授权金额是否小于电子现金重置阈值）以确定是否进行后续的安全性信息交互过程，并且如果确定进行后续的安全性信息交互过程，则向所述用户终端传送回安全性信息交互批准应答，以及如果确定不需进行后续的安全性信息交互过程，则向所述用户终端传送回安全性信息交互拒绝应答。

优选地，在本发明所公开的安全性信息交互方法中，所述步骤（A6）进一步包括：在接收到来自所述数据处理服务器的认证结果通知后，所述用户终端执行如下操作：如果所述认证结果通知是安全性信息交互拒绝应答，则提示用户安全性信息交互失败，并且如果所述认证结果通知是安全性信息交互批准应答，则执行与当前进行的安全性信息交互过程相关联的数据处理操作（例如对电子现金进行扣款）并生成所述安全性信息交互数据，以及将所述安全性信息交互数据传送到所述数据处理服务器。

优选地，在本发明所公开的安全性信息交互方法中，所述安全性信息交互数据包括安全性信息交互凭证（例如交易扣款凭证）和其他与当前进行的安全性信息交互过程相关联的信息（例如安全性信息交互标识符，诸如订单号）。

优选地，在本发明所公开的安全性信息交互方法中，所述步骤（A7）进一步包括：所述数据处理服务器验证所述安全性信息交互凭证。

优选地，在本发明所公开的安全性信息交互方法中，所述安全性信息交互装置是所述网络中的节点（即可以通过所述网络与外部设备进行数据通信）。

优选地，在本发明所公开的安全性信息交互方法中，通过 SSL 协议

实现所述安全性信息交互装置与所述数据处理服务器之间的数据通信。

优选地，在本发明所公开的安全性信息交互方法中，通过 SSL 协议实现所述用户终端与所述数据处理服务器之间的数据通信。

优选地，在本发明所公开的安全性信息交互方法中，通过对称密钥体系实现所述认证过程。

优选地，在本发明所公开的安全性信息交互方法中，所述步骤（A6）进一步包括：以加密的方式传送所述安全性信息交互数据（其包括安全性信息交互凭证），其中，将安全性信息交互标识符（诸如订单号）作为加密密钥的生成因子。

示例性地，在本发明所公开的安全性信息交互方法中，所述智能卡可以是 SIM 卡，或智能 SD 卡，或终端附件等。

优选地，在本发明所公开的安全性信息交互方法中，所述步骤（A4）进一步包括：所述用户终端以如下方式从脱机应用获取所述应用数据：（1）向所述智能卡发送选择脱机应用的指令以选择脱机应用；（2）初始化所述脱机应用；（3）提示用户输入针对所述脱机应用的 PIN（个人识别码）从而验证用户的身份，并且如果验证通过，则执行后续操作，而如果验证未通过，则提示重新输入所述针对所述脱机应用的 PIN，并重复验证过程，以及如果输入次数超过预定的阈值则提示用户身份验证失败；向所述脱机应用发送读取应用数据指令以获取所述应用数据。

示例性地，在金融领域中，所述与当前进行的安全性信息交互过程相关联的数据处理操作可以是为了完成交易而对电子现金进行的扣款操作，并且具体的操作过程可以如下：所述用户终端向所述智能卡发送扣款请求；收到扣款请求后，所述智能卡执行卡片风险分析以决定是否批准该交易请求；如果批准，则返回脱机交易批准密文 TC，此时卡内的电子现金金额已经进行了更新；如果不批准，则返回拒绝响应（例如密文 AAC）；用户终端判断是否为脱机交易批准 TC 密文，并且如果是，则组装脱机交易扣款凭证，并将该凭证发送给所述智能卡进行加密和 MAC 计算；所述智能卡确认该脱机交易扣款凭证确实属于本帐户的有效脱机交易数据（即未经处理过的属于本帐户的脱机交易数据），则完成相关的安全操

作，而如果确认不是，则返回错误指示。

由上可见，本发明所公开的安全性信息交互方法具有如下优点：（1）能够应用于脱机方式的远程信息交互；（2）由于使用了多种安全措施（例如，以加密的方式传送安全性信息交互数据，其中，将安全性信息交互标识符（诸如订单号）作为加密密钥的生成因子），故具有高的安全性。

尽管本发明是通过上述的优选实施方式进行描述的，但是其实现形式并不局限于上述的实施方式。应该认识到：在不脱离本发明主旨和范围的情况下，本领域技术人员可以对本发明做出不同的变化和修改。

权利要求

1. 一种安全性信息交互方法，所述安全性信息交互方法包括下列步骤：

（A1）用户终端将来自用户的安全性信息交互指令通过网络传送到远程安全性信息交互装置；

（A2）所述安全性信息交互装置接收来自所述用户终端的所述安全性信息交互指令，并基于所述安全性信息交互指令构造安全性信息交互请求以及将所述安全性信息交互请求传送到数据处理服务器；

（A3）所述数据处理服务器接收并解析来自所述安全性信息交互装置的所述安全性信息交互请求，并基于所述安全性信息交互请求向所述用户终端发送安全性信息交互确认请求；

（A4）所述用户终端接收来自所述数据处理服务器的所述安全性信息交互确认请求，以及基于所述安全性信息交互确认请求从智能卡中的脱机应用获取应用数据并将所述应用数据传送到所述数据处理服务器；

（A5）所述数据处理服务器接收所述用户终端传送回的所述应用数据，并基于所述应用数据执行认证操作以及将认证结果通知传送回所述用户终端；

（A6）所述用户终端接收来自所述数据处理服务器的认证结果通知，并基于所述认证结果通知生成安全性信息交互数据以及将所述安全性信息交互数据传送到所述数据处理服务器；

（A7）所述数据处理服务器接收来自所述用户终端的所述安全性信息交互数据，并基于所述安全性信息交互数据执行验证操作以及将与验证结果相关的消息传送到所述安全性信息交互装置。

2. 根据权利要求1所述的安全性信息交互方法，其特征在于，所述步骤（A7）进一步包括：如果所述验证结果是“验证成功”，则所述数据处理服务器向所述用户终端发送安全性信息交互成功应答。

3. 根据权利要求2所述的安全性信息交互方法，其特征在于，所述步骤（A7）进一步包括：如果所述验证结果是“验证成功”，则所述数据

处理服务器将与验证结果相关的通知发送到业务提供方服务器。

4. 根据权利要求3所述的安全性信息交互方法，其特征在于，所述用户终端是移动终端中的客户端，并且所述网络是移动通信网络。

5. 根据权利要求4所述的安全性信息交互方法，其特征在于，所述应用数据包括脱机认证数据和用于终端风险管理和行为分析的数据。

6. 根据权利要求5所述的安全性信息交互方法，其特征在于，所述步骤（A5）进一步包括：在接收到所述用户终端传送回的所述应用数据后，所述数据处理服务器执行如下操作：解析所述应用数据以获得脱机认证数据和用于终端风险管理和行为分析的数据；基于所述脱机认证数据执行认证操作，并且如果认证结果为“认证未通过”，则向所述用户终端传送回安全性信息交互拒绝应答；如果认证结果为“认证通过”，则执行终端风险管理和行为分析操作以确定是否进行后续的安全性信息交互过程，并且如果确定进行后续的安全性信息交互过程，则向所述用户终端传送回安全性信息交互批准应答，以及如果确定不需进行后续的安全性信息交互过程，则向所述用户终端传送回安全性信息交互拒绝应答。

7. 根据权利要求6所述的安全性信息交互方法，其特征在于，所述步骤（A6）进一步包括：在接收到来自所述数据处理服务器的认证结果通知后，所述用户终端执行如下操作：如果所述认证结果通知是安全性信息交互拒绝应答，则提示用户安全性信息交互失败，并且如果所述认证结果通知是安全性信息交互批准应答，则执行与当前进行的安全性信息交互过程相关联的数据处理操作并生成所述安全性信息交互数据，以及将所述安全性信息交互数据传送到所述数据处理服务器。

8. 根据权利要求7所述的安全性信息交互方法，其特征在于，所述安全性信息交互数据包括安全性信息交互凭证和其他与当前进行的安全性信息交互过程相关联的信息。

9. 根据权利要求8所述的安全性信息交互方法，其特征在于，所述步骤（A7）进一步包括：所述数据处理服务器验证所述安全性信息交互凭证。

10. 根据权利要求9所述的安全性信息交互方法，其特征在于，通过

SSL 协议实现所述安全性信息交互装置与所述数据处理服务器之间的数据通信。

11. 根据权利要求10所述的安全性信息交互方法，其特征在于，通过 SSL 协议实现所述用户终端与所述数据处理服务器之间的数据通信。

12. 根据权利要求11所述的安全性信息交互方法，其特征在于，所述步骤（A6）进一步包括：以加密的方式传送所述安全性信息交互数据，其中，将安全性信息交互标识符作为加密密钥的生成因子。

13. 根据权利要求12所述的安全性信息交互方法，其特征在于，所述步骤（A4）进一步包括：所述用户终端以如下方式从脱机应用获取所述应用数据：（1）向所述智能卡发送选择脱机应用的指令以选择脱机应用；（2）初始化所述脱机应用；（3）提示用户输入针对所述脱机应用的 PIN 从而验证用户的身份，并且如果验证通过，则执行后续操作，而如果验证未通过，则提示重新输入所述针对所述脱机应用的 PIN，并重复验证过程，以及如果输入次数超过预定的阈值则提示用户身份验证失败；向所述脱机应用发送读取应用数据指令以获取所述应用数据。

14. 一种安全性信息交互系统，所述安全性信息交互系统包括：

至少一个用户终端，所述至少一个用户终端中的每个用于将来自用户的安全性信息交互指令通过网络传送到远程安全性信息交互装置，并接收来自数据处理服务器的安全性信息交互确认请求，以及基于所述安全性信息交互确认请求从脱机应用获取应用数据并将所述应用数据传送到所述数据处理服务器，所述至少一个用户终端中的每个进一步用于接收来自所述数据处理服务器的认证结果通知，并基于所述认证结果通知生成安全性信息交互数据以及将所述安全性信息交互数据传送到所述数据处理服务器；

安全性信息交互装置，所述安全性信息交互装置用于接收来自所述用户终端的所述安全性信息交互指令，并基于所述安全性信息交互指令构造安全性信息交互请求以及将所述安全性信息交互请求传送到所述数据处理服务器；

数据处理服务器，所述数据处理服务器用于接收并解析来自所述安

全性信息交互装置的所述安全性信息交互请求，并基于所述安全性信息交互请求向相应的用户终端发送所述安全性信息交互确认请求，所述数据处理服务器进一步用于接收所述用户终端传送回的应用数据，并基于所述应用数据执行认证操作以及将认证结果通知传送回相应的用户终端，所述数据处理服务器进一步用于接收来自所述用户终端的所述安全性信息交互数据，并基于所述安全性信息交互数据执行验证操作以及将与验证结果相关的消息传送到所述安全性信息交互装置；

智能卡，所述智能卡用于存储至少一个脱机应用。

15．一种用户终端，所述用户终端将来自用户的安全性信息交互指令通过网络传送到远程安全性信息交互装置，并接收来自数据处理服务器的安全性信息交互确认请求，以及基于所述安全性信息交互确认请求从智能卡中的脱机应用获取应用数据并将所述应用数据传送到所述数据处理服务器，所述用户终端进一步用于接收来自所述数据处理服务器的认证结果通知，并基于所述认证结果通知生成安全性信息交互数据以及将所述安全性信息交互数据传送到所述数据处理服务器。

16．一种数据处理服务器，所述数据处理服务器接收并解析来自安全性信息交互装置的安全性信息交互请求，并基于所述安全性信息交互请求向相应的用户终端发送安全性信息交互确认请求，所述数据处理服务器进一步用于接收所述用户终端传送回的应用数据，并基于所述应用数据执行认证操作以及将认证结果通知传送回相应的用户终端，所述数据处理服务器进一步用于接收来自所述用户终端的安全性信息交互数据，并基于所述安全性信息交互数据执行验证操作以及将与验证结果相关的消息传送到所述安全性信息交互装置。

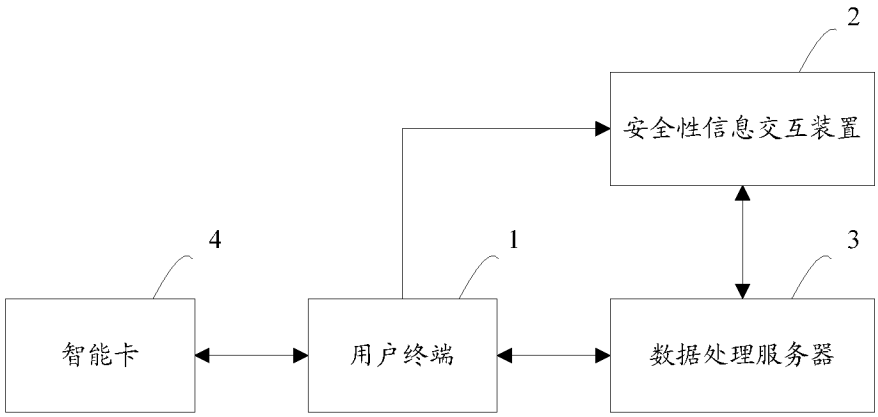


图 1

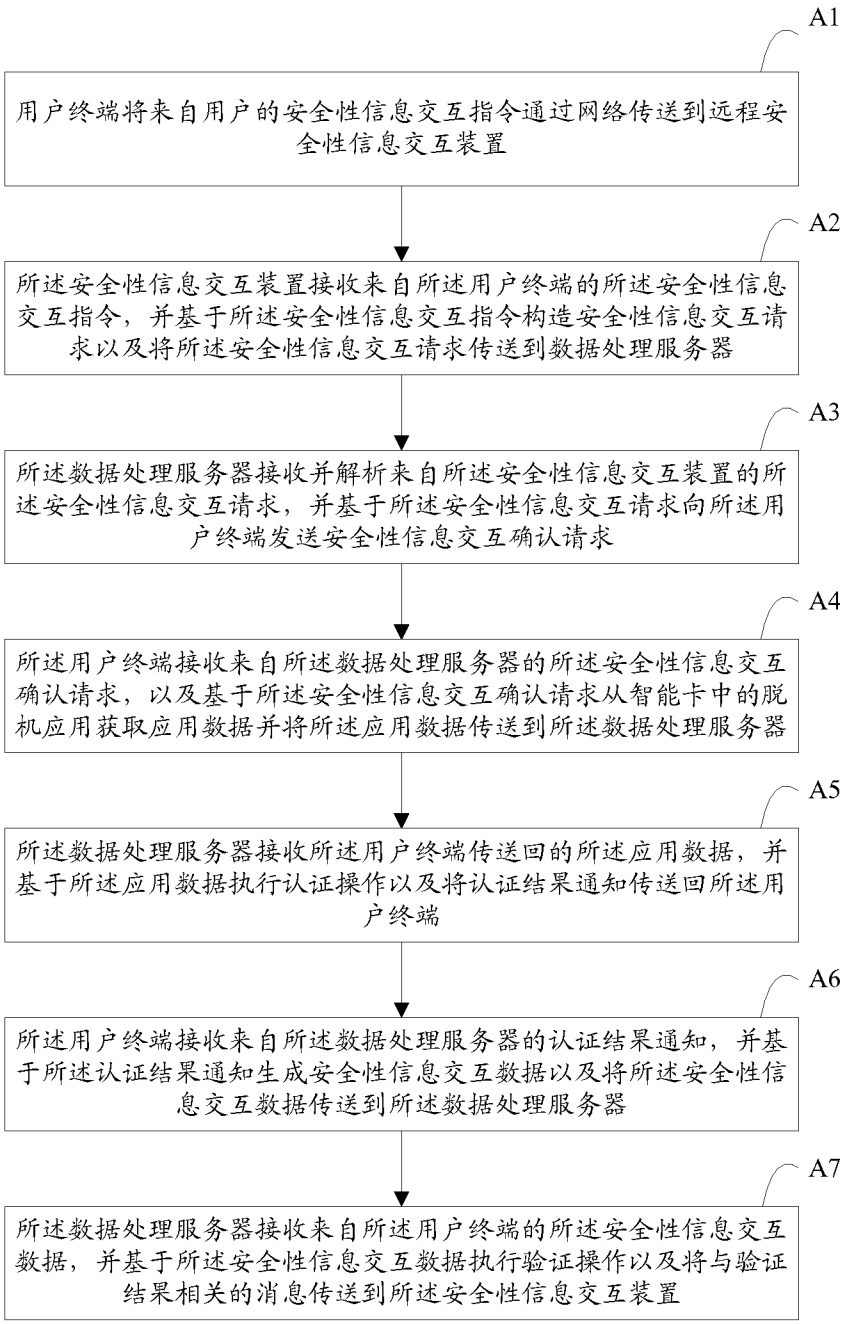

A1
用户终端将来自用户的安全性信息交互指令通过网络传送到远程安全性信息交互装置
A2
所述安全性信息交互装置接收来自所述用户终端的所述安全性信息交互指令，并基于所述安全性信息交互指令构造安全性信息交互请求以及将所述安全性信息交互请求传送到数据处理服务器
A3
所述数据处理服务器接收并解析来自所述安全性信息交互装置的所述安全性信息交互请求，并基于所述安全性信息交互请求向所述用户终端发送安全性信息交互确认请求
A4
所述用户终端接收来自所述数据处理服务器的所述安全性信息交互确认请求，以及基于所述安全性信息交互确认请求从智能卡中的脱机应用获取应用数据并将所述应用数据传送到所述数据处理服务器
A5
所述数据处理服务器接收所述用户终端传送回的所述应用数据，并基于所述应用数据执行认证操作以及将认证结果通知传送回所述用户终端
A6
所述用户终端接收来自所述数据处理服务器的认证结果通知，并基于所述认证结果通知生成安全性信息交互数据以及将所述安全性信息交互数据传送到所述数据处理服务器
A7
所述数据处理服务器接收来自所述用户终端的所述安全性信息交互数据，并基于所述安全性信息交互数据执行验证操作以及将与验证结果相关的消息传送到所述安全性信息交互装置

图 2

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2013/084183

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06 (2006.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC: H04W, H04Q, H04L, H04M, G06Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

IEEE, WPL, EPODOC, CNPAT, CNKI: instruction, POS machine, safe information, interactive, verify, authentication, off-line, remote, long distance, pay, buy, purchase, order, mobile phone, mobile terminal, server, POS

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 102419846 A (99BILL PAYMENT AND SETTLEMENT INFORMATION CO., LTD.), 18 April 2012 (18.04.2012), description, paragraphs 0047-0053, and figure 3	1-16
A	CN 101394615 A (CHINA UNIONPAY CO., LTD.), 25 March 2009 (25.03.2009), abstract, and abstract figure	1-16
A	CN 101923757 A (SHENZHEN INSTITUTES OF ADVANCED TECHNOLOGY, CHINESE ACADEMY OF SCIENCES), 22 December 2010 (22.12.2010), the whole document	1-16
A	US 2002/0038287 A1 (VILLARET, J.M. et al.), 28 March 2002 (28.03.2002), the whole document	1-16

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
06 December 2013 (06.12.2013)	**26 December 2013 (26.12.2013)**
Name and mailing address of the ISA/CN: State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No.: (86-10) 62019451	Authorized officer **SHANG, Xiaoli** Telephone No.: (86-10) **62413395**

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2013/084183

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 102419846 A	18.04.2012	None	
CN 101394615 A	25.03.2009	WO 2009039771 A1	02.04.2009
		CN 101394615 B	17.10.2012
CN 101923757 A	22.12.2010	None	
US 2002/0038287 A1	28.03.2002	JP 2003108902 A	11.04.2003
		EP 1271435 A2	02.01.2003

国际检索报告

国际申请号
PCT/CN2013/084183

A. 主题的分类

H04L 29/06 (2006.01) i

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

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

IPC: H04W, H04Q, H04L, H04M, G06Q

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）)

IEEE,WPI,EPODOC,CNPAT,CNKI:安全信息，交互，验证，指令，认证，脱机，远程，支付，购买，订单，手机，移动终端，服务器，POS 机，safe information, interactive, verify, authentication, off-line, remote, long distance, pay, buy, purchase, order, mobile phone, mobile terminal, server, POS

C. 相关文件

类　型*	引用文件，必要时，指明相关段落	相关的权利要求
A	CN 102419846 A (快钱支付清算信息有限公司) 18.4 月 2012 (18.04.2012) 说明书第 0047-0053 段，附图 3	1-16
A	CN 101394615 A (中国银联股份有限公司) 25.3 月 2009 (25.03.2009) 说明书摘要，摘要附图	1-16
A	CN 101923757 A (中国科学院深圳先进技术研究院) 22.12 月 2010 (22.12.2010) 全文	1-16
A	US2002/0038287 A1 (VILLARET Jean-Marc 等) 28.3 月 2002 (28.03.2002) 全文	1-16

☐ 其余文件在 C 栏的续页中列出。　　☒ 见同族专利附件。

* 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	国际检索报告邮寄日期
06.12 月 2013 (06.12.2013)	**26.12 月 2013 (26.12.2013)**
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 商晓莉 电话号码：(86-10) **62413395**

国际检索报告

关于同族专利的信息

国际申请号 **PCT/CN2013/084183**

检索报告中引用的专利文件	公布日期	同族专利	公布日期
CN 102419846 A	18.04.2012	无	
CN 101394615 A	25.03.2009	WO 2009039771 A1	02.04.2009
		CN 101394615 B	17.10.2012
CN 101923757 A	22.12.2010	无	
US 2002/0038287 A1	28.03.2002	JP 2003108902 A	11.04.2003
		EP 1271435 A2	02.01.2003