

(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 1 月 3 日 (03.01.2014)



(10) 国际公布号
WO 2014/000601 A1

- (51) 国际专利分类号:
G06F 21/00 (2013.01)
- (21) 国际申请号: PCT/CN2013/077649
- (22) 国际申请日: 2013 年 6 月 21 日 (21.06.2013)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201210214595.1 2012 年 6 月 27 日 (27.06.2012) CN
- (71) 申请人: 中国银联股份有限公司 (CHINA UNION-PAY 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: 程志强 (CHENG, Zhiqiang); 中国上海市含笑路 36 号银联大厦 7 楼, Shanghai 200135 (CN)。王海冰 (WANG, Haibing); 中国上海市含笑路 36 号银联大厦 7 楼, Shanghai 200135 (CN)。何朔 (HE,

Shuo); 中国上海市含笑路 36 号银联大厦 7 楼, Shanghai 200135 (CN)。鲁志军 (LU, Zhijun); 中国上海市含笑路 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, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV,

[见续页]

(54) Title: SECURITY INFORMATION INTERACTION SYSTEM, DEVICE AND METHOD

(54) 发明名称: 安全性信息交互系统、设备及方法

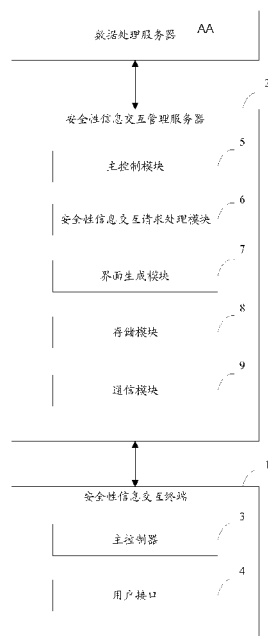


图 1 / Fig. 1

- 1 Security information interaction terminal
- 2 Security information interaction management server
- 3 Main controller
- 4 User interface
- 5 Main control module
- 6 Security information interaction request processing module
- 7 Interface generation module
- 8 Storage module
- 9 Communication module
- AA Data processing server

(57) Abstract: A security information interaction system, device and method. The security information interaction system comprises a security information interaction terminal (1) and a security information interaction management server (2), wherein the security information interaction terminal (1) is used for acquiring from the security information interaction management server (2) a main application interface and a security information interaction interface and displaying same based on a security information interaction instruction from a user, and constructing a security information interaction request based on the security information inputted by the user through the security interaction interface and sending the security information interaction request to the security information interaction management server (2). The abovementioned security information interaction system, device and method are easy to use and maintain, and low in cost.

(57) 摘要: 安全性信息交互系统、设备及方法。其中, 安全性信息交互系统包括安全性信息交互终端 (1) 和安全性信息交互管理服务器 (2), 所述安全性信息交互终端 (1) 用于基于来自用户的安全性信息交互指令从安全性信息交互管理服务器 (2) 获取并显示应用主界面和安全性信息交互界面, 以及基于用户通过所述安全性交互界面输入的安全性信息构造安全性信息交互请求, 并将所述安全性信息交互请求发送到所述安全性信息交互管理服务器 (2)。上述安全性信息交互系统、设备及方法易于使用和维护, 并且成本较低。



SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC,
VN, ZA, ZM, ZW。

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)。

- (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,

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，通过安全性信息交互终端（例如 POS 机）并经由网络进行安全性信息（即对安全性要求较高的信息，例如交易金额和/或密码）的交互变得越来越重要。

现有的安全性信息交互系统及方法通常采用常规的安全性信息交互终端（例如常规的 POS 机）。然而，常规的安全性信息交互终端存在如下问题：（1）更新和安装应用困难，从而导致维护成本较高；（2）针对新的应用，需要兼容不同平台的安全性信息交互终端，从而导致设计和调试成本较高。

因此，存在如下需求：提供易于使用和维护并且成本较低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所存在的问题，本发明提出了易于使用和维护并且成本较低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系统，所述安全性信息交互系统包括：

安全性信息交互终端，所述安全性信息交互终端用于基于来自用户的安全性信息交互指令从安全性信息交互管理服务器获取并显示应用主界面和安全性信息交互界面，以及基于用户通过所述安全性信息交互界面输入的安全性信息构造安全性信息交互请求，并将所述安全性信息交互请求发送到所述安全性信息交互管理服务器；

安全性信息交互管理服务器，所述安全性信息交互管理服务器用于为所述安全性信息交互终端提供所述应用主界面和所述安全性信息交互界面，以及解

析和处理接收到的所述安全性信息交互请求以完成安全性信息交互过程,并将处理结果传送回所述安全性信息交互终端。

在上面所公开的方案中,优选地,所述安全性信息交互终端是 B/S 模式中的浏览器。

- 5 在上面所公开的方案中,优选地,所述安全性信息交互终端进一步用于显示来自所述安全性信息交互管理服务器的所述处理结果。

在上面所公开的方案中,优选地,所述安全性信息交互终端进一步包括:

- 10 用户接口,所述用户接口用于接收来自用户的安全性信息交互指令并将所述安全性信息交互指令传送到主控制器,以及显示所述应用主界面和所述安全性信息交互界面并接收用户输入的所述安全性信息,以及将所述安全性信息传送到主控制器,所述用户接口还用于显示来自所述安全性信息交互管理服务器的所述处理结果;

- 15 主控制器,所述主控制器用于基于接收到的所述安全性信息交互指令从所述安全性信息交互管理服务器获取所述应用主界面和所述安全性信息交互界面以通过所述用户接口显示,以及基于接收到的所述安全性信息构造所述安全性信息交互请求,并将所述安全性信息交互请求发送到所述安全性信息交互管理服务器。

- 20 在上面所公开的方案中,优选地,所述主控制器通过请求 URL 的方式从所述安全性信息交互管理服务器获取所述应用主界面和所述安全性信息交互界面,其中,所述应用主界面和所述安全性信息交互界面是 HTML 页面的形式。

- 25 在上面所公开的方案中,优选地,在用户通过由所述用户接口显示的所述应用主界面输入安全性信息交互类型信息后,所述主控制器基于所述安全性信息交互类型信息通过请求 URL 的方式从所述安全性信息交互管理服务器获取所述安全性信息交互界面,其中,所述安全性信息交互界面包含安全性信息交互处理逻辑和该处理逻辑所需的数据。

在上面所公开的方案中,优选地,所述主控制器按照所述安全性信息交互处理逻辑处理用户通过由所述用户接口显示的所述安全性信息交互界面输入的所述安全性信息以构造所述安全性信息交互请求,并将所述安全性信息交互请求以 HTTP 报文的方式传送到所述安全性信息交互管理服务器,其中,所述

安全性信息交互请求包含对安全性信息交互的类型的指示。

在上面所公开的方案中，优选地，所述安全性信息交互管理服务器进一步包括：

主控制模块，所述主控制模块用于接收来自所述安全性信息交互终端的应用主界面 URL 请求和安全性信息交互界面 URL 请求，并将所述应用主界面 URL 请求和安全性信息交互界面 URL 请求传送到界面生成模块，以及接收并解析来自所述安全性信息交互终端的所述安全性信息交互请求，并将解析后的安全性信息交互请求传送到安全性信息交互请求处理模块；

界面生成模块，所述界面生成模块用于基于接收到的所述应用主界面 URL 请求生成应用主界面并将所述应用主界面传送回所述安全性信息交互终端，以及基于接收到的所述安全性信息交互界面 URL 请求生成安全性信息交互界面并将所述安全性信息交互界面传送回所述安全性信息交互终端，其中，所述安全性信息交互界面 URL 请求包含所述安全性信息交互类型信息；

安全性信息交互请求处理模块，所述安全性信息交互请求处理模块用于处理接收到的所述解析后的安全性信息交互请求，并通过与数据处理服务器的数据交互完成安全性信息交互过程，并将处理结果传送回所述安全性信息交互终端，其中，当所述安全性信息交互请求指示安全性信息交互的类型为“脱机方式”时，所述安全性信息交互请求处理模块将所述安全性信息交互请求所包含的安全性信息交互数据存储在存储模块中；

存储模块，所述存储模块用于至少存储所述安全性信息交互数据；

通信模块，所述通信模块用于执行所述安全性信息交互管理服务器与所述安全性信息交互终端和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，所述主控制模块进一步用于在解析所述安全性信息交互请求之前对所述安全性信息交互终端的合法性进行认证，并且将解析后的安全性信息交互请求通过路由的方式传送到所述安全性信息交互请求处理模块。

在上面所公开的方案中，优选地，当接收到的所述安全性信息交互请求指示安全性信息交互的类型为“联机方式”时，所述安全性信息交互请求处理模块基于所述安全性信息交互请求以预定格式构造安全性信息交互报文，随后以

加密的方式将所述安全性信息交互报文传送到所述数据处理服务器以进行后续处理，以及将所述数据处理服务器传送回的处理结果以 HTML 页面的形式传送到所述安全性信息交互终端。

在上面所公开的方案中，优选地，当接收到的所述安全性信息交互请求指示安全性信息交互的类型为“脱机方式”时，所述安全性信息交互请求处理模块将所述安全性信息交互请求所包含的安全性信息交互数据存储在所述存储模块中，并将处理结果以 HTML 页面的形式传送回所述安全性信息交互终端。

在上面所公开的方案中，优选地，所述安全性信息交互请求处理模块周期性地将存储在所述存储模块中的未处理的安全性信息交互数据以批量地方式传送到所述数据处理服务器以进行后续的处理。

在上面所公开的方案中，优选地，在所述安全性信息交互终端与所述安全性信息交互管理服务器之间以安全通道的方式进行通信，并且以 HTML 超文本的方式进行相互之间的数据传输。

在上面所公开的方案中，优选地，所述主控制模块进一步用于统一管理所述安全性信息交互终端。

本发明的目的也可以通过以下技术方案实现：

一种安全性信息交互终端，所述安全性信息交互终端用于基于来自用户的安全性信息交互指令从安全性信息交互管理服务器获取并显示应用主界面和安全性信息交互界面，以及基于用户通过所述安全性信息交互界面输入的安全性信息构造安全性信息交互请求，并将所述安全性信息交互请求发送到所述安全性信息交互管理服务器。

本发明的目的也可以通过以下技术方案实现：

一种安全性信息交互管理服务器，所述安全性信息交互管理服务器用于为安全性信息交互终端提供应用主界面和安全性信息交互界面，以及解析和处理接收到的来自所述安全性信息交互终端的安全性信息交互请求以完成安全性信息交互过程，并将处理结果传送回所述安全性信息交互终端。

本发明的目的也可以通过以下技术方案实现：

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) 安全性信息交互终端基于来自用户的安全性信息交互指令从安全性

信息交互管理服务器获取并显示应用主界面；

(A2) 在用户通过所述应用主界面输入安全性信息交互类型信息后，所述安全性信息交互终端基于所述安全性信息交互类型信息通过请求 URL 的方式从所述安全性信息交互管理服务器获取并显示安全性信息交互界面，其中，所述安全性信息交互界面包含安全性信息交互处理逻辑和该处理逻辑所需的数据；

(A3) 基于用户通过所述安全性信息交互界面输入的安全性信息构造安全性信息交互请求，并将所述安全性信息交互请求发送到所述安全性信息交互管理服务器；

10 (A4) 所述安全性信息交互管理服务器解析和处理接收到的所述安全性信息交互请求以完成安全性信息交互过程，并将处理结果传送回所述安全性信息交互终端。

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：由于采用了 B/S 模式，故将在常规的安全性信息交互终端中执行的处理逻辑转移到安全性信息交互管理服务器中执行，故易于使用和维护并且成本较低。

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：

20 图1是根据本发明的实施例的安全性信息交互系统的架构图；

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架构图。如图1所示，
25 本发明所公开的安全性信息交互系统包括安全性信息交互终端1和安全性信息交互管理服务器2（示例性地，所述安全性信息交互管理服务器2可以是金融领域中的 POS 终端后台系统）。其中，所述安全性信息交互终端1用于基于来自用户的安全性信息交互指令从安全性信息交互管理服务器2获取并显示应用主界面和安全性信息交互界面，以及基于用户通过所述安全性信息交互界面输入

的安全性信息构造安全性信息交互请求（其中，所述安全性信息交互请求包括所述安全性信息交互终端1的标识符），并将所述安全性信息交互请求发送到所述安全性信息交互管理服务器2。所述安全性信息交互管理服务器2用于为所述安全性信息交互终端1提供所述应用主界面和所述安全性信息交互界面，以及解析和处理接收到的所述安全性信息交互请求以完成安全性信息交互过程，并将处理结果传送回所述安全性信息交互终端1。

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终端1是 B/S 模式中的浏览器（示例性地，所述浏览器位于移动终端、或个人计算机、或 POS 机中，并且可以示例性地但不限于运行在 Window CE、或 Android、或 Linux 操作系统平台上）。

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管理服务器2是 B/S 模式中的服务器。

优选地，在本发明所公开的安全性信息交互系统中，所述安全性信息交互终端1进一步用于显示来自所述安全性信息交互管理服务器2的所述处理结果。

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终端1进一步包括主控制器3和用户接口4。其中，所述用户接口4用于接收来自用户的安全性信息交互指令并将所述安全性信息交互指令传送到主控制器3，以及显示所述应用主界面和所述安全性信息交互界面并接收用户输入的所述安全性信息（示例性地，所述安全性信息可以包括交易类型、消费金额、磁道信息或智能卡信息等），以及将所述安全性信息传送到主控制器3，所述用户接口4还用于显示来自所述安全性信息交互管理服务器2的所述处理结果。所述主控制器3用于基于接收到的所述安全性信息交互指令从所述安全性信息交互管理服务器2获取所述应用主界面和所述安全性信息交互界面以通过所述用户接口4显示，以及基于接收到的所述安全性信息构造所述安全性信息交互请求，并将所述安全性信息交互请求发送到所述安全性信息交互管理服务器2。

优选地，在本发明所公开的安全性信息交互系统中，所述主控制器3通过请求 URL 的方式从所述安全性信息交互管理服务器2获取所述应用主界面和所述安全性信息交互界面，其中，所述应用主界面和所述安全性信息交互界面是 HTML 页面的形式。

优选地，在本发明所公开的安全性信息交互系统中，在用户通过由所述用户接口4显示的所述应用主界面输入安全性信息交互类型信息（示例性地，在金融领域中，安全性信息交互类型可以是“余额查询”、“消费”、“圈存”等）后，所述主控制器3基于所述安全性信息交互类型信息通过请求 URL 的方式从所述安全性信息交互管理服务器2获取所述安全性信息交互界面，其中，所述安全性信息交互界面包含安全性信息交互处理逻辑和该处理逻辑所需的数据（示例性地，以 JavaScript 的方式提供所述安全性信息交互处理逻辑）。

优选地，在本发明所公开的安全性信息交互系统中，所述主控制器3按照所述安全性信息交互处理逻辑处理用户通过由所述用户接口4显示的所述安全性信息交互界面输入的所述安全性信息（例如将数据打包）以构造所述安全性信息交互请求，并将所述安全性信息交互请求以 HTTP 报文的方式传送到所述安全性信息交互管理服务器2，其中，所述安全性信息交互请求包含对安全性信息交互的类型的指示（即“联机方式”或“脱机方式”）。

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管理服务器2进一步包括主控制模块5、安全性信息交互请求处理模块6、界面生成模块7、存储模块8和通信模块9。其中，所述主控制模块5用于接收来自所述安全性信息交互终端1的应用主界面 URL 请求和安全性信息交互界面 URL 请求，并将所述应用主界面 URL 请求和安全性信息交互界面 URL 请求传送到界面生成模块7，以及接收并解析来自所述安全性信息交互终端1的所述安全性信息交互请求，并将解析后的安全性信息交互请求传送到安全性信息交互请求处理模块6。所述界面生成模块7用于基于接收到的所述应用主界面 URL 请求生成应用主界面并将所述应用主界面传送回所述安全性信息交互终端1，以及基于接收到的所述安全性信息交互界面 URL 请求生成安全性信息交互界面（优选地，所述安全性信息交互界面包含安全性信息交互处理逻辑和该处理逻辑所需的数据）并将所述安全性信息交互界面传送回所述安全性信息交互终端1，其中，所述安全性信息交互界面 URL 请求包含所述安全性信息交互类型信息。所述安全性信息交互请求处理模块6用于处理接收到的所述解析后的安全性信息交互请求，并通过与数据处理服务器（示例性地，该数据处理服务器可以是金融领域中的金融收单平台）的数据交互完成安全性信息交互过程，并将处理结果传

送回所述安全性信息交互终端1（示例性地，所述处理结果以 HTML 页面的形式被传送到所述安全性信息交互终端1），其中，当所述安全性信息交互请求指示安全性信息交互的类型为“脱机方式”时，所述安全性信息交互请求处理模块6将所述安全性信息交互请求所包含的安全性信息交互数据（例如交易信息，其可以包括交易类型、交易时间、交易金额等）存储在存储模块8中。所述存储模块8用于至少存储所述安全性信息交互数据。所述通信模块9用于执行所述安全性信息交互管理服务器2与所述安全性信息交互终端1和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系统中，主控制模块5进一步用于在解析所述安全性信息交互请求之前对所述安全性信息交互终端1的合法性进行认证，并且将解析后的安全性信息交互请求通过路由的方式（例如交易路由）传送到所述安全性信息交互请求处理模块6。

优选地，在本发明所公开的安全性信息交互系统中，当接收到的所述安全性信息交互请求指示安全性信息交互的类型为“联机方式”时，所述安全性信息交互请求处理模块6基于所述安全性信息交互请求以预定格式构造安全性信息交互报文，随后以加密的方式将所述安全性信息交互报文传送到所述数据处理服务器以进行后续处理，以及将所述数据处理服务器传送回的处理结果以 HTML 页面的形式传送到所述安全性信息交互终端1。

优选地，在本发明所公开的安全性信息交互系统中，当接收到的所述安全性信息交互请求指示安全性信息交互的类型为“脱机方式”时，所述安全性信息交互请求处理模块6将所述安全性信息交互请求所包含的安全性信息交互数据（例如交易信息，其可以包括交易类型、交易时间、交易金额等）存储在所述存储模块8中，并将处理结果以 HTML 页面的形式传送到所述安全性信息交互终端1。

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请求处理模块6周期性地将在所述存储模块8中的未处理的安全性信息交互数据（其与“脱机方式”的安全性信息交互相关联）以批量地方式传送到所述数据处理服务器以进行后续的处理。

优选地，在本发明所公开的安全性信息交互系统中，在所述安全性信息交

互终端1与所述安全性信息交互管理服务器2之间采用安全通道进行通信,并且以 HTML 超文本的方式进行相互之间的数据传输(即在所述安全性信息交互终端1与所述安全性信息交互管理服务器2之间采用 HTTP 协议传输数据)。

优选地,在本发明所公开的安全性信息交互系统中,所述主控制模块5进一步用于统一管理所述安全性信息交互终端1(示例性地,本发明所公开的安全性信息交互系统包含多个安全性信息交互终端1)。示例性地,所述管理包括下列中的至少一项:终端操作员管理、多级权限管理策略、终端参数管理(示例性地,终端参数可以包括终端编号、商户编号、终端最低限额等)。

如图1所示,本发明公开了一种安全性信息交互终端1,所述安全性信息交互终端1用于基于来自用户的安全性信息交互指令从安全性信息交互管理服务器获取并显示应用主界面和安全性信息交互界面,以及基于用户通过所述安全性信息交互界面输入的安全性信息构造安全性信息交互请求(其中,所述安全性信息交互请求包括所述安全性信息交互终端1的标识符),并将所述安全性信息交互请求发送到所述安全性信息交互管理服务器。

15 优选地,本发明所公开的安全性信息交互终端1是 B/S 模式中的浏览器(示例性地,所述浏览器位于移动终端、或个人计算机、或 POS 机中,并且可以示例性地但不限于运行在 Window CE、或 Android、或 Linux 操作系统平台上)。

优选地,本发明所公开的安全性信息交互终端1进一步用于显示来自所述安全性信息交互管理服务器2的处理结果。

20 优选地,本发明所公开的安全性信息交互终端1进一步包括主控制器3和用户接口4。其中,所述用户接口4用于接收来自用户的安全性信息交互指令并将所述安全性信息交互指令传送到主控制器3,以及显示所述应用主界面和所述安全性信息交互界面并接收用户输入的所述安全性信息(示例性地,所述安全性信息可以包括交易类型、消费金额、磁道信息或智能卡信息等),以及将所述安全性信息传送到主控制器3,所述用户接口4还用于显示来自所述安全性信息交互管理服务器2的所述处理结果。所述主控制器3用于基于接收到的所述安全性信息交互指令从所述安全性信息交互管理服务器2获取所述应用主界面和所述安全性信息交互界面以通过所述用户接口4显示,以及基于接收到的所述安全性信息构造所述安全性信息交互请求,并将所述安全性信息交互请求发送

25

到所述安全性信息交互管理服务器2。

优选地，在本发明所公开的安全性信息交互终端1中，所述主控制器3通过请求 URL 的方式从所述安全性信息交互管理服务器2获取所述应用主界面和所述安全性信息交互界面，其中，所述应用主界面和所述安全性信息交互界面是
5 HTML 页面的形式。

优选地，在本发明所公开的安全性信息交互终端1中，在用户通过由所述用户接口4显示的所述应用主界面输入安全性信息交互类型信息（示例性地，在金融领域中，安全性信息交互类型可以是“余额查询”、“消费”、“圈存”等）后，所述主控制器3基于所述安全性信息交互类型信息通过请求 URL 的方式从所述安全性信息交互管理服务器2获取所述安全性信息交互界面，其中，
10 所述安全性信息交互界面包含安全性信息交互处理逻辑和该处理逻辑所需的数据（示例性地，以 JavaScript 的方式提供所述安全性信息交互处理逻辑）。

优选地，在本发明所公开的安全性信息交互终端1中，所述主控制器3按照所述安全性信息交互处理逻辑处理用户通过由所述用户接口4显示的所述安全性信息交互界面输入的所述安全性信息（例如将数据打包）以构造所述安全性信息交互请求，并将所述安全性信息交互请求以 HTTP 报文的方式传送到所述安全性信息交互管理服务器2，其中，所述安全性信息交互请求包含对安全性信息交互的类型的指示（即“联机方式”或“脱机方式”）。

优选地，本发明所公开的安全性信息交互终端1采用安全通道的方式进行与
20 所述安全性信息交互管理服务器2的通信，并且以 HTML 超文本的方式进行相互之间的数据传输（即在所述安全性信息交互终端1与所述安全性信息交互管理服务器2之间采用 HTTP 协议传输数据）。

如图1所示，本发明公开了一种安全性信息交互管理服务器2，所述安全性信息交互管理服务器2用于为安全性信息交互终端1提供应用主界面和安全性信息交互界面，以及解析和处理接收到的来自所述安全性信息交互终端1的安全性信息交互请求以完成安全性信息交互过程，并将处理结果传送回所述安全性信息交互终端1。
25

优选地，本发明所公开的安全性信息交互管理服务器2是 B/S 模式中的服务器。

优选地，本发明所公开的安全性信息交互管理服务器2进一步包括主控制模块5、安全性信息交互请求处理模块6、界面生成模块7、存储模块8和通信模块9。其中，所述主控制模块5用于接收来自所述安全性信息交互终端1的应用主界面 URL 请求和安全性信息交互界面 URL 请求，并将所述应用主界面 URL 请求和安全性信息交互界面 URL 请求传送到界面生成模块7，以及接收并解析来自所述安全性信息交互终端1的所述安全性信息交互请求，并将解析后的安全性信息交互请求传送到安全性信息交互请求处理模块6。所述界面生成模块7用于基于接收到的所述应用主界面 URL 请求生成应用主界面并将所述应用主界面传送回所述安全性信息交互终端1，以及基于接收到的所述安全性信息交互界面 URL 请求生成安全性信息交互界面（优选地，所述安全性信息交互界面包含安全性信息交互处理逻辑和该处理逻辑所需的数据）并将所述安全性信息交互界面传送回所述安全性信息交互终端1，其中，所述安全性信息交互界面 URL 请求包含所述安全性信息交互类型信息。所述安全性信息交互请求处理模块6用于处理接收到的所述解析后的安全性信息交互请求，并通过与数据处理服务器（示例性地，该数据处理服务器可以是金融领域中的金融收单平台）的数据交互完成安全性信息交互过程，并将处理结果传送回所述安全性信息交互终端1（示例性地，所述处理结果以 HTML 页面的形式被传送回所述安全性信息交互终端1），其中，当所述安全性信息交互请求指示安全性信息交互的类型为“脱机方式”时，所述安全性信息交互请求处理模块6将所述安全性信息交互请求所包含的安全性信息交互数据（例如交易信息，其可以包括交易类型、交易时间、交易金额等）存储在存储模块8中。所述存储模块8用于至少存储所述安全性信息交互数据。所述通信模块9用于执行所述安全性信息交互管理服务器2与所述安全性信息交互终端1和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管理服务器2中，所述主控制模块5进一步用于在解析所述安全性信息交互请求之前对所述安全性信息交互终端1的合法性进行认证，并且将解析后的安全性信息交互请求通过路由的方式（例如交易路由）传送到所述安全性信息交互请求处理模块6。

优选地，在本发明所公开的安全性信息交互管理服务器2中，当接收到的所述安全性信息交互请求指示安全性信息交互的类型为“联机方式”时，所述

安全性信息交互请求处理模块6基于所述安全性信息交互请求以预定格式构造安全性信息交互报文,随后以加密的方式将所述安全性信息交互报文传送到所述数据处理服务器以进行后续处理,以及将所述数据处理服务器传送回的处理结果以 HTML 页面的形式传送到所述安全性信息交互终端1。

5 优选地,在本发明所公开的安全性信息交互管理服务器2中,当接收到的所述安全性信息交互请求指示安全性信息交互的类型为“脱机方式”时,所述安全性信息交互请求处理模块6将所述安全性信息交互请求所包含的安全性信息交互数据(例如交易信息,其可以包括交易类型、交易时间、交易金额等)存储在所述存储模块8中,并将处理结果以 HTML 页面的形式传送回所述安全性
10 信息交互终端1。

优选地,在本发明所公开的安全性信息交互管理服务器2中,所述安全性信息交互请求处理模块6周期性地将存储在所述存储模块8中的未处理的安全性信息交互数据(其与“脱机方式”的安全性信息交互相关联)以批量地方式传送到所述数据处理服务器以进行后续的处理。

15 优选地,本发明所公开的安全性信息交互管理服务器2与所述安全性信息交互终端1之间以安全通道的方式进行通信,并且以 HTML 超文本的方式进行相互之间的数据传输(即在所述安全性信息交互终端1与所述安全性信息交互管理服务器2之间采用 HTTP 协议传输数据)。

20 优选地,在本发明所公开的安全性信息交互管理服务器2中,所述主控制模块5进一步用于统一管理所述安全性信息交互终端1(示例性地,本发明所公开的安全性信息交互管理服务器2管理多个安全性信息交互终端1)。示例性地,所述管理包括下列中的至少一项:终端操作员管理、多级权限管理策略、终端参数管理(示例性地,终端参数可以包括终端编号、商户编号、终端最低限额等)。

25 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)安全性信息交互终端基于来自用户的安全性信息交互指令从安全性信息交互管理服务器(示例性地,所述安全性信息交互管理服务器可以是金融领域中的 POS 终端后台系统)获取并显示应用主界面;(A2)在用户通过所述应用主界面输入安全性信息交

互类型信息（示例性地，在金融领域中，安全性信息交互类型可以是“余额查询”、“消费”、“圈存”等）后，所述安全性信息交互终端基于所述安全性信息交互类型信息通过请求 URL 的方式从所述安全性信息交互管理服务器获取并显示安全性信息交互界面，其中，所述安全性信息交互界面包含安全性信息交互处理逻辑和该处理逻辑所需的数据（示例性地，以 JavaScript 的方式提供所述安全性信息交互处理逻辑）；（A3）基于用户通过所述安全性信息交互界面输入的安全性信息构造安全性信息交互请求（其中，所述安全性信息交互请求包括所述安全性信息交互终端1的标识符），并将所述安全性信息交互请求发送到所述安全性信息交互管理服务器；（A4）所述安全性信息交互管理服务器解析和处理接收到的所述安全性信息交互请求以完成安全性信息交互过程，并将处理结果传送回所述安全性信息交互终端。

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终端是 B/S 模式中的浏览器（示例性地，所述浏览器位于移动终端、或个人计算机、或 POS 机中，并且可以示例性地但不限于运行在 Window CE、或 Android、或 Linux 操作系统平台上）。

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管理服务器是 B/S 模式中的服务器。

优选地，在本发明所公开的安全性信息交互方法中，所述步骤（A4）进一步包括：所述安全性信息交互终端显示来自所述安全性信息交互管理服务器的所述处理结果。

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终端通过请求 URL 的方式从所述安全性信息交互管理服务器获取所述应用主界面和所述安全性信息交互界面，其中，所述应用主界面和所述安全性信息交互界面是 HTML 页面的形式。

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（A3）进一步包括：所述安全性信息交互终端按照所述安全性信息交互处理逻辑处理用户通过所述安全性信息交互界面输入的所述安全性信息（例如将数据打包）以构造所述安全性信息交互请求，并将所述安全性信息交互请求以 HTTP 报文的方式传送到所述安全性信息交互管理服务器，其中，所述安全性信息交互请求包

含对安全性信息交互的类型的指示（即“联机方式”或“脱机方式”）。

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（A1）进一步包括：所述安全性信息交互管理服务器基于接收到的应用主界面 URL 请求生成应用主界面并将所述应用主界面传送给所述安全性信息交互终端。

5 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（A2）进一步包括：所述安全性信息交互管理服务器基于接收到的安全性信息交互界面 URL 请求生成安全性信息交互界面（优选地，所述安全性信息交互界面包含安全性信息交互处理逻辑和该处理逻辑所需的数据）并将所述安全性信息交互界面传送给所述安全性信息交互终端，其中，所述安全性信息交互界面 URL 请求
10 包含所述安全性信息交互类型信息。

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：所述安全性信息交互管理服务器处理并解析接收到的所述安全性信息交互请求，并通过与数据处理服务器（示例性地，该数据处理服务器可以是金融领域中的金融收单平台）的数据交互完成安全性信息交互过程，并将处理结果
15 传送给所述安全性信息交互终端（示例性地，所述处理结果以 HTML 页面的形式被传送给所述安全性信息交互终端）。

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：所述安全性信息交互管理服务器在解析所述安全性信息交互请求之前对所述安全性信息交互终端的合法性进行认证。

20 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：当接收到的所述安全性信息交互请求指示安全性信息交互的类型为“联机方式”时，所述安全性信息交互管理服务器基于所述安全性信息交互请求以预定格式构造安全性信息交互报文，随后以加密的方式将所述安全性信息交互报文传送到所述数据处理服务器以进行后续处理，以及将所述数据处理服务器传送回的处理结果以 HTML 页面的形式传送到所述安全性信息交互终端。
25

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：当接收到的所述安全性信息交互请求指示安全性信息交互的类型为“脱机方式”时，所述安全性信息交互管理服务器存储所述安全性信息交互请求所包含的安全性信息交互数据（例如交易信息，其可以包括交易类型、交易

时间、交易金额等)，并将处理结果以 HTML 页面的形式传送回所述安全性信息交互终端。

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管理服务器周期性地将存储的未处理的安全性信息交互数据(其与“脱机方式”的安全性信息交互相关联)以批量地方式传送到所述数据处理服务器以进行后续的处理。

优选地，在本发明所公开的安全性信息交互方法中，在所述安全性信息交互终端与所述安全性信息交互管理服务器之间采用安全通道的方式进行通信，并且以 HTML 超文本的方式进行相互之间的数据传输(即在所述安全性信息交互终端与所述安全性信息交互管理服务器之间采用 HTTP 协议传输数据)。

优选地，在本发明所公开的安全性信息交互方法中，所述安全性信息交互管理服务器统一管理所述安全性信息交互终端(示例性地，本发明所公开的安全性信息交互方法包含多个安全性信息交互终端)。示例性地，所述管理包括下列中的至少一项：终端操作员管理、多级权限管理策略、终端参数管理(示例性地，终端参数可以包括终端编号、商户编号、终端最低限额等)。

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。

20

25

权利要求

1. 一种安全性信息交互系统，所述安全性信息交互系统包括：

安全性信息交互终端，所述安全性信息交互终端用于基于来自用户的安全性信息交互指令从安全性信息交互管理服务器获取并显示应用主界面和安全性信息交互界面，以及基于用户通过所述安全性信息交互界面输入的安全性信息构造安全性信息交互请求，并将所述安全性信息交互请求发送到所述安全性信息交互管理服务器；

安全性信息交互管理服务器，所述安全性信息交互管理服务器用于为所述安全性信息交互终端提供所述应用主界面和所述安全性信息交互界面，以及解析和处理接收到的所述安全性信息交互请求以完成安全性信息交互过程，并将处理结果传送回所述安全性信息交互终端。

2. 根据权利要求1所述的安全性信息交互系统，其特征在于，所述安全性信息交互终端是 B/S 模式中的浏览器。

3. 根据权利要求2所述的安全性信息交互系统，其特征在于，所述安全性信息交互终端进一步用于显示来自所述安全性信息交互管理服务器的所述处理结果。

4. 根据权利要求3所述的安全性信息交互系统，其特征在于，所述安全性信息交互终端进一步包括：

用户接口，所述用户接口用于接收来自用户的安全性信息交互指令并将所述安全性信息交互指令传送到主控制器，以及显示所述应用主界面和所述安全性信息交互界面并接收用户输入的所述安全性信息，以及将所述安全性信息传送到主控制器，所述用户接口还用于显示来自所述安全性信息交互管理服务器的所述处理结果；

主控制器，所述主控制器用于基于接收到的所述安全性信息交互指令从所述安全性信息交互管理服务器获取所述应用主界面和所述安全性信息交互界面以通过所述用户接口显示，以及基于接收到的所述安全性信息构造所述安全性信息交互请求，并将所述安全性信息交互请求发送到所述安全性信息交互管理服务器。

5. 根据权利要求4所述的安全性信息交互系统，其特征在于，所述主控制器通过请求 URL 的方式从所述安全性信息交互管理服务器获取所述应用主界面和所述安全性信息交互界面，其中，所述应用主界面和所述安全性信息交互界面是 HTML 页面的形式。

5 6. 根据权利要求5所述的安全性信息交互系统，其特征在于，在用户通过由所述用户接口显示的所述应用主界面输入安全性信息交互类型信息后，所述主控制器基于所述安全性信息交互类型信息通过请求 URL 的方式从所述安全性信息交互管理服务器获取所述安全性信息交互界面，其中，所述安全性信息交互界面包含安全性信息交互处理逻辑和该
10 处理逻辑所需的数据。

7. 根据权利要求6所述的安全性信息交互系统，其特征在于，所述主控制器按照所述安全性信息交互处理逻辑处理用户通过由所述用户接口显示的所述安全性信息交互界面输入的所述安全性信息以构造所述安全性信息交互请求，并将所述安全性信息交互请求以 HTTP 报文的方式
15 传送到所述安全性信息交互管理服务器，其中，所述安全性信息交互请求包含对安全性信息交互的类型的指示。

8. 根据权利要求7所述的安全性信息交互系统，其特征在于，所述安全性信息交互管理服务器进一步包括：

主控制模块，所述主控制模块用于接收来自所述安全性信息交互终端的应用主界面 URL 请求和安全性信息交互界面 URL 请求，并将所述应用主界面 URL 请求和安全性信息交互界面 URL 请求传送到界面生成模块，以及接收并解析来自所述安全性信息交互终端的所述安全性信息交互请求，并将解析后的安全性信息交互请求传送到安全性信息交互请求处理模块；
20

25 界面生成模块，所述界面生成模块用于基于接收到的所述应用主界面 URL 请求生成应用主界面并将所述应用主界面传送回所述安全性信息交互终端，以及基于接收到的所述安全性信息交互界面 URL 请求生成安全性信息交互界面并将所述安全性信息交互界面传送回所述安全性信息交互终端，其中，所述安全性信息交互界面 URL 请求包含所述安全性信

息交互类型信息;

安全性信息交互请求处理模块, 所述安全性信息交互请求处理模块用于处理接收到的所述解析后的安全性信息交互请求, 并通过与数据处理服务器的数据交互完成安全性信息交互过程, 并将处理结果传送到所述安全性信息交互终端, 其中, 当所述安全性信息交互请求指示安全性信息交互的类型为“脱机方式”时, 所述安全性信息交互请求处理模块将所述安全性信息交互请求所包含的安全性信息交互数据存储在存储模块中;

存储模块, 所述存储模块用于至少存储所述安全性信息交互数据;

10 通信模块, 所述通信模块用于执行所述安全性信息交互管理服务器与所述安全性信息交互终端和所述数据处理服务器之间的数据通信。

9. 根据权利要求8所述的安全性信息交互系统, 其特征在于, 所述主控制模块进一步用于在解析所述安全性信息交互请求之前对所述安全性信息交互终端的合法性进行认证, 并且将解析后的安全性信息交互请求通过路由的方式传送到所述安全性信息交互请求处理模块。

10. 根据权利要求9所述的安全性信息交互系统, 其特征在于, 当接收到的所述安全性信息交互请求指示安全性信息交互的类型为“联机方式”时, 所述安全性信息交互请求处理模块基于所述安全性信息交互请求以预定格式构造安全性信息交互报文, 随后以加密的方式将所述安全性信息交互报文传送到所述数据处理服务器以进行后续处理, 以及将所述数据处理服务器传送回的处理结果以 HTML 页面的形式传送到所述安全性信息交互终端。

11. 根据权利要求10所述的安全性信息交互系统, 其特征在于, 当接收到的所述安全性信息交互请求指示安全性信息交互的类型为“脱机方式”时, 所述安全性信息交互请求处理模块将所述安全性信息交互请求所包含的安全性信息交互数据存储在所述存储模块中, 并将处理结果以 HTML 页面的形式传送到所述安全性信息交互终端。

12. 根据权利要求11所述的安全性信息交互系统, 其特征在于, 所述安全性信息交互请求处理模块周期性地将存储在所述存储模块中的未

处理的安全性信息交互数据以批量地方式传送到所述数据处理服务器以进行后续的处理。

13. 根据权利要求12所述的安全性信息交互系统，其特征在于，在所述安全性信息交互终端与所述安全性信息交互管理服务器之间以安全通道的方式进行通信，并且以 HTML 超文本的方式进行相互之间的数据传输。

14. 根据权利要求13所述的安全性信息交互系统，其特征在于，所述主控制模块进一步用于统一管理所述安全性信息交互终端。

15. 一种安全性信息交互终端，所述安全性信息交互终端用于基于来自用户的安全性信息交互指令从安全性信息交互管理服务器获取并显示应用主界面和安全性信息交互界面，以及基于用户通过所述安全性信息交互界面输入的安全性信息构造安全性信息交互请求，并将所述安全性信息交互请求发送到所述安全性信息交互管理服务器。

16. 一种安全性信息交互管理服务器，所述安全性信息交互管理服务器用于为安全性信息交互终端提供应用主界面和安全性信息交互界面，以及解析和处理接收到的来自所述安全性信息交互终端的安全性信息交互请求以完成安全性信息交互过程，并将处理结果传送回所述安全性信息交互终端。

17. 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) 安全性信息交互终端基于来自用户的安全性信息交互指令从安全性信息交互管理服务器获取并显示应用主界面；

(A2) 在用户通过所述应用主界面输入安全性信息交互类型信息后，所述安全性信息交互终端基于所述安全性信息交互类型信息通过请求 URL 的方式从所述安全性信息交互管理服务器获取并显示安全性信息交互界面，其中，所述安全性信息交互界面包含安全性信息交互处理逻辑和该处理逻辑所需的数据；

(A3) 基于用户通过所述安全性信息交互界面输入的安全性信息构造安全性信息交互请求，并将所述安全性信息交互请求发送到所述安全性

信息交互管理服务器;

(A4) 所述安全性信息交互管理服务器解析和处理接收到的所述安全性信息交互请求以完成安全性信息交互过程, 并将处理结果传送回所述安全性信息交互终端。

5

10

15

20

25

1/2

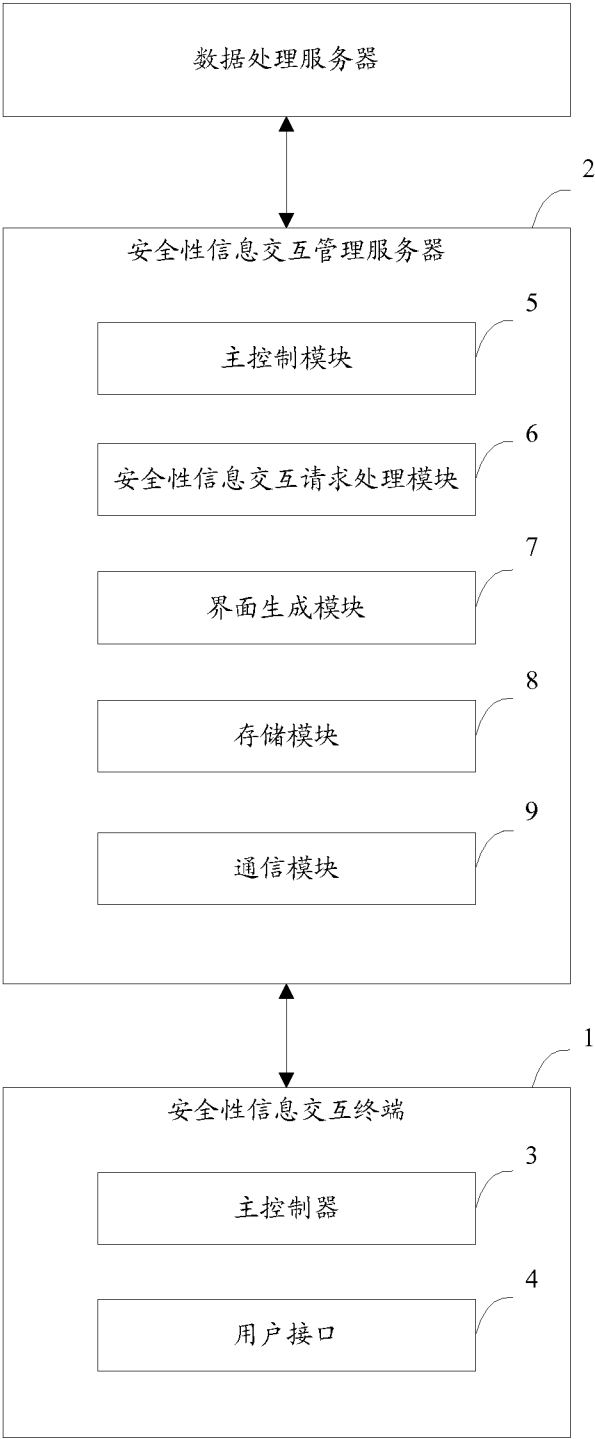


图 1

2/2

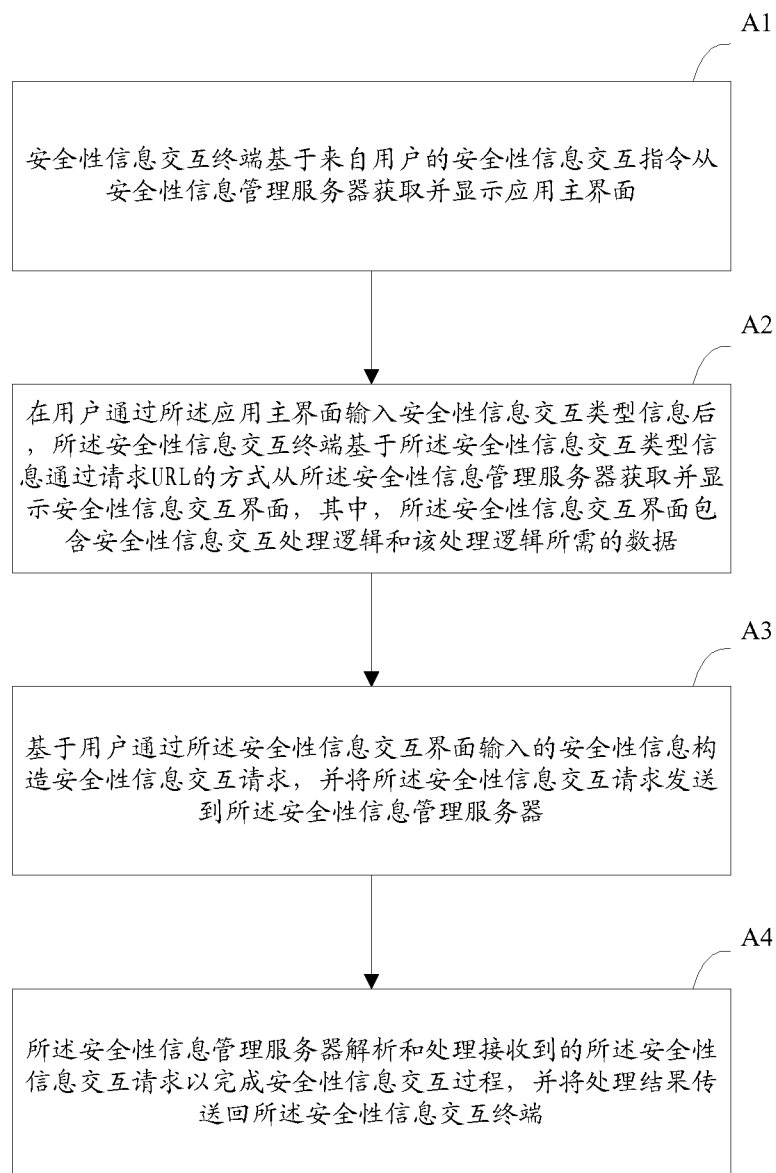


图 2

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2013/077649

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/00 (2013.01) 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: G06F 21/-

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)

CNPAT, CNKI, WPI, EPODOC: safe, security, communication, terminal, server, dictate, request, interface, browser

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 101938520 A (ZTE CORP.) 05 January 2011 (05.01.2011) see description, paragraph [0053] to paragraph [0059], claims 1 to 14 and figure 1	1-17
A	CN 102368780 A (QIZHI SOFTWARE BEIJING CO LTD) 07 March 2012 (07.03.2012) see the whole document	1-17
A	CN 102255924 A (ZHEJIANG CHINA TOBACCO IND CO) 23 November 2011 (23.11.2011) see the whole document	1-17

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:	“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
“A” document defining the general state of the art which is not considered to be of particular relevance	“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
“E” earlier application or patent but published on or after the international filing date	“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
“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)	“&” document member of the same patent family
“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	

Date of the actual completion of the international search 13 September 2013 (13.09.2013)	Date of mailing of the international search report 10 October 2013 (10.10.2013)
Name and mailing address of the ISA 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 ZHAO, Jing Telephone No. (86-10) 62411884

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2013/077649

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 101938520 A	05.01.2011	WO 2012031433 A	15.03.2012
		US 2013166456 A	27.06.2013
		EP 2518670 A1	31.10.2012
CN 102368780 A	07.03.2012	CN 102368780 B	20.03.2013
CN 102255924 A	23.11.2011	None	

国际检索报告

国际申请号

PCT/CN2013/077649

A. 主题的分类

G06F 21/00 (2013.01) 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: G06F 21/-

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))

CNPAT,CNKI,WPI,EPODOC: 安全, 信息, 交互, 通信, 终端, 服务器, 指令, 请求, 界面, 接口, 浏览器; safe, security, communication, terminal, server, dictate, request, interface, browser

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
X	CN101938520A (中兴通讯股份有限公司) 05.1 月 2011(05.01.2011) 参见说明书第 53 段至 59 段、权利要求 1-14、图 1	1-17
A	CN102368780A (奇智软件(北京)有限公司) 07.3 月 2012(07.03.2012)参见全文	1-17
A	CN102255924A (浙江中烟工业有限责任公司) 23.11 月 2011(23.11.2011) 参见全文	1-17

☐ 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
13.9 月 2013 (13.09.2013)

国际检索报告邮寄日期
10.10 月 2013 (10.10.2013)

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

授权官员

赵婧
电话号码: (86-10) **62411884**

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2013/077649

检索报告中引用的 专利文件	公布日期	同族专利	公布日期
CN101938520A	05.01.2011	WO2012031433A	15.03.2012
		US2013166456A	27.06.2013
		EP2518670A1	31.10.2012
CN102368780A	07.03.2012	CN102368780B	20.03.2013
CN102255924A	23.11.2011	无	