

(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
2018 年 6 月 7 日 (07.06.2018)



(10) 国际公布号
WO 2018/099209 A1

(51) 国际专利分类号:
H04L 29/08 (2006.01)

(21) 国际申请号: PCT/CN2017/107454

(22) 国际申请日: 2017 年 10 月 24 日 (24.10.2017)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201611076397.8 2016 年 11 月 29 日 (29.11.2016) 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: 郭弘强(GUO, Hongqiang); 中国上海市浦东新区含笑路 36 号银联大厦, Shanghai 200135 (CN)。 李伟(LI, Wei); 中国上海市浦东新区含笑路 36 号银联大厦, Shanghai 200135 (CN)。 唐真(TANG, Zhen); 中国上海市浦东新区含笑路 36 号银联大厦, Shanghai 200135 (CN)。

(74) 代理人: 北京同达信恒知识产权代理有限公司 (TDIP & PARTNERS); 中国北京市海淀区宝盛南路 1 号院 20 号楼 8 层 101-01, Beijing 100192 (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, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK,

(54) Title: STANDARDISATION METHOD AND APPARATUS FOR ERRONEOUS TRANSACTIONS

(54) 发明名称: 一种差错交易的标准化方法及装置

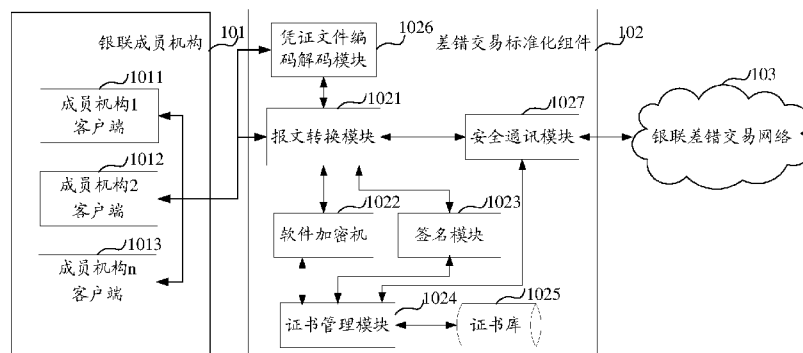


图 1

- 101 UNIONPAY MEMBER INSTITUTIONS
- 102 ERRONEOUS TRANSACTION STANDARDISATION ASSEMBLY
- 103 UNIONPAY ERRONEOUS TRANSACTION NETWORK
- 1011 MEMBER INSTITUTION 1 CLIENT TERMINAL
- 1012 MEMBER INSTITUTION 2 CLIENT TERMINAL
- 1013 MEMBER INSTITUTION N CLIENT TERMINAL
- 1021 MESSAGE CONVERSION MODULE
- 1022 SOFTWARE ENCRYPTION MACHINE
- 1023 SIGNATURE MODULE
- 1024 CERTIFICATE MANAGEMENT MODULE
- 1025 CERTIFICATE DATABASE
- 1026 CREDENTIALS FILE ENCODING AND DECODING MODULE
- 1027 SECURE COMMUNICATION MODULE

(57) Abstract: Disclosed in the present invention are a standardisation method and apparatus for erroneous transactions: receiving an erroneous service invocation request sent by a client terminal, and converting the erroneous service invocation request into a standard format exchange message; on the basis of a preset certificate database, encrypting sensitive data areas in the exchange message to generate encrypted message areas; signing key fields in the exchange message to generate signed message areas; and, by means of a two-way authenticated secure communication link, sending the exchange message comprising the encrypted message areas and

LR, LS, 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, 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, ST, 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))。

the signed message areas to a UnionPay erroneous transaction network. The embodiments of the present invention provide a unified interface for interfacing client terminals to access a UnionPay erroneous transaction network; each UnionPay member institution only needs to invoke the interface assembly provided in the embodiments of the present invention to be able to interface with the UnionPay erroneous transaction network, improving development efficiency and operating stability.

(57) 摘要: 本发明公开了一种差错交易的标准化方法及装置, 通过接收客户端发送的差错业务调用请求, 将所述差错业务调用请求转换为标准格式的交换报文; 根据预设的证书库, 对所述交换报文中的敏感数据域进行加密, 生成加密报文域; 以及对所述交换报文中的关键字段进行签名, 生成签名报文域; 通过双向认证的安全通讯链路将包含所述加密报文域和所述签名报文域的交换报文发送至银联差错交易网络。本发明实施例提供了接入银联差错交易网络对接客户端的统一接口, 各银联成员机构只需调用本发明实施例提供的接口组件, 即可实现与银联差错交易网络的对接, 提高了开发效率和运行稳定性。

一种差错交易的标准化方法及装置

本申请要求在 2016 年 11 月 29 日提交中国专利局、申请号为 201611076397.8、发明名称为“一种差错交易的标准化方法及装置”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本发明涉及互联网领域，尤其涉及一种差错交易的标准化方法及装置。

背景技术

随着互联网技术的发展，银行卡支付途径也因此多元化。银行卡支付过程涉及到收单机构、银行卡组织、发卡机构等多方参与，一旦在支付过程中出现异常导致机构间账务出现差错，需要各方通过传递、审核大量的交易信息和凭证文件来证实账务的真实情况。

银联差错交易网络是全球银联成员机构的银行卡差错业务处理网络，即各成员机构联机处理差错交易的统一信息交换网络，该网络的核心是银联差错服务系统，成员机构通过各自建设差错对接客户端来接入该网络。由于银联差错业务规则和技术规范复杂、交易网络安全标准较高，而成员机构技术水平有限、客户端的运行环境各不相同，导致机构接入端的开发周期长、测试问题多、运行出错率高等问题，大大增加了成员机构接入银联差错交易网络的成本，降低了成员机构接入银联差错交易网络的效率。

此外，现有的成员机构建设的接入银联差错对接网络的客户端系统，都是基于自身的实现技术、系统环境和接入需求开发的，对本机构的运行环境依赖性较高，且缺少通用的开发接口，运行稳定性较差，因此只能供本机构接入差错对接网络使用，无法适用于其它成员机构。

综上所述，亟需一种跨平台标准组件来统一各成员机构与银联差错交易网络的对接。

发明内容

本发明提供一种差错交易的标准化方法及装置，用以解决现有技术中银联成员机构与银联差错交易网络之间缺少通用的开发接口，运行稳定性较差，开发效率低的问题。

第一方面，本发明实施例提供一种差错交易的标准化方法，包括：

接收客户端发送的差错业务调用请求，将所述差错业务调用请求转换为标准格式的交换报文；

根据预设的证书库，对所述交换报文中的敏感数据域进行加密，生成加密报文域；以及对所述交换报文中的关键字段进行签名，生成签名报文域；

通过双向认证的安全通讯链路将包含所述加密报文域和所述签名报文域的交换报文发送至银联差错交易网络。

较佳地，所述标准格式的交换报文包括可扩展标记语言 XML 报文标签名称和 XML 报文标签值，所述将所述差错业务调用请求转换为标准格式的交换报文，包括：

根据预设的调用方法名称与报文标签的对应关系，将所述差错业务调用请求的调用方法名称转化成 XML 报文标签名称；

将所述差错业务调用请求的调用方法参数转化成 XML 报文标签的值。

较佳地，所述预设的证书库通过以下方式确定：

提取中国金融认证中心 CFCA 的非对称加密证书中的服务器公钥和客户端私钥，通过所述服务器公钥和客户端私钥确定所述预设证书库，所述 CFCA 的非对称加密证书用于接入银联差错交易网络。

较佳地，所述根据预设的证书库，对所述差错业务调用请求的敏感数据域进行加密，生成加密报文域，包括：

调用所述预设证书库中的服务器公钥，对所述差错业务调用请求的敏感数据域进行加密，生成加密报文域。

较佳地，所述差错业务调用请求中的关键字段进行签名，生成签名报文

域, 包括:

调用所述预设证书库中的客户端私钥, 对所述差错业务调用请求中的关键字段进行签名, 生成签名报文域。

较佳地, 所述双向认证的安全通讯链路通过以下方式确定:

调用所述预设证书库中的服务器公钥和客户端私钥, 根据安全套接层上的超文本传输协议 HTTPS, 建立与所述银联差错交易网络的双向认证的安全通讯链路。

较佳地, 所述通过安全通讯链路将包含所述加密报文域和所述签名报文域的所述交换报文发送至银联差错交易网络之前, 还包括:

若所述差错业务调用请求中包括二进制编码形式的凭证文件, 则对所述凭证文件进行解码;

通过所述银联差错交易网络的编码方式对所解码后的凭证文件进行编码。

第二方面, 本发明实施例还提供一种差错交易的标准化装置, 包括:

格式转换单元: 用于接收客户端发送的差错业务调用请求, 将所述差错业务调用请求转换为标准格式的交换报文;

报文域转换单元: 用于根据预设的证书库, 对所述交换报文中的敏感数据域进行加密, 生成加密报文域; 以及对所述交换报文中的关键字段进行签名, 生成签名报文域;

发送单元: 用于通过双向认证的安全通讯链路将包含所述加密报文域和所述签名报文域的交换报文发送至银联差错交易网络。

较佳地, 所述标准格式的交换报文包括可扩展标记语言 XML 报文标签名称和 XML 报文标签值, 所述格式转换单元, 具体用于:

根据预设的调用方法名称与报文标签的对应关系, 将所述差错业务调用请求的调用方法名称转化成 XML 报文标签名称;

将所述差错业务调用请求的调用方法参数转化成 XML 报文标签的值。

较佳地, 所述预设的证书库通过以下方式确定:

提取中国金融认证中心 CFCA 的非对称加密证书中的服务器公钥和客户端私钥，通过所述服务器公钥和客户端私钥确定所述预设证书库，所述 CFCA 的非对称加密证书用于接入银联差错交易网络。

较佳地，所述报文域转换单元，具体用于：

调用所述预设证书库中的服务器公钥，对所述差错业务调用请求的敏感数据域进行加密，生成加密报文域。

较佳地，所述报文域转换单元，具体用于：

调用所述预设证书库中的客户端私钥，对所述差错业务调用请求中的关键字段进行签名，生成签名报文域。

较佳地，所述双向认证的安全通讯链路通过以下方式确定：

调用所述预设证书库中的服务器公钥和客户端私钥，根据安全套接层上的超文本传输协议 HTTPS，建立与所述银联差错交易网络的双向认证的安全通讯链路。

较佳地，所述报文域转换单元，还用于：

若所述差错业务调用请求中包括二进制编码形式的凭证文件，则对所述凭证文件进行解码；

通过所述银联差错交易网络的编码方式对所解码后的凭证文件进行编码。

第三方面，本发明实施例提供一种电子设备，包括：处理器、存储器、收发机、总线接口，其中处理器、存储器与收发机之间通过总线接口连接；

所述收发机，用于接收客户端发送的差错业务调用请求；

所述处理器，用于读取所述存储器中的程序，执行下列方法：将所述差错业务调用请求转换为标准格式的交换报文；根据预设的证书库，对所述交换报文中的敏感数据域进行加密，生成加密报文域；以及对所述交换报文中的关键字段进行签名，生成签名报文域；通过双向认证的安全通讯链路将包含所述加密报文域和所述签名报文域的交换报文发送至银联差错交易网络；

所述存储器，用于存储一个或多个可执行程序，可以存储所述处理器在

执行操作时所使用的数据；

所述收发机还用于将所述风险等级发送给交易平台，以使交易平台根据所述风险等级确定是否进行支付；

所述总线接口，用于提供接口。

第四方面，本发明实施例提供一种非暂态计算机可读存储介质，所述非暂态计算机可读存储介质存储计算机指令，所述计算机指令用于使所述计算机执行上述第一方面中任一实施例所述差错交易的标准化方法。

第五方面，本发明实施例提供一种计算机程序产品，所述计算机程序产品包括存储在非暂态计算机可读存储介质上的计算程序，所述计算机程序包括程序指令，当所述程序指令被计算机执行时，使所述计算机执行上述第一方面中任一实施例所述差错交易的标准化方法。

本发明实施例提供的差错交易的标准化方法及装置，通过接收客户端发送的差错业务调用请求，将所述差错业务调用请求转换为标准格式的交换报文；根据预设的证书库，对所述交换报文中的敏感数据域进行加密，生成加密报文域；以及对所述交换报文中的关键字段进行签名，生成签名报文域；通过双向认证的安全通讯链路将包含所述加密报文域和所述签名报文域的交换报文发送至银联差错交易网络。本发明实施例提供了接入银联差错交易网络对接客户端的统一接口，各银联成员机构只需调用本发明实施例提供的接口组件，即可实现与银联差错交易网络的对接，提高了开发效率和运行稳定性。

附图说明

为了更清楚地说明本发明实施例中的技术方案，下面将对实施例描述中所需要使用的附图作简要介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域的普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

图1为本发明实施例提供的一种差错交易的标准化系统结构示意图；

图 2 为本发明实施例提供的一种差错交易的标准化方法流程示意图；

图 3 为本发明实施例提供的一种差错交易的标准化装置结构示意图；

图 4 为本发明实施例提供的一种电子设备的结构示意图。

具体实施方式

为了使本发明的目的、技术方案和优点更加清楚，下面将结合附图对本发明作进一步地详细描述，显然，所描述的实施例仅仅是本发明一部份实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其它实施例，都属于本发明保护的范围。

本发明实施例提供一种差错交易的标准化系统，如图 1 所示，为本发明实施例提供的一种差错交易的标准化系统结构示意图。包括银联成员机构 101、差错交易标准化组件 102、银联差错交易网络 103。其中，银联成员机构包括：成员机构 1 客户端 1011，成员机构 2 客户端 1012，成员机构 n 客户端 1013，银联成员机构 101 通过各自的客户端调用本发明实施例提供的差错交易标准化组件 102，即可实现与银联差错交易网络 103 的对接。

本发明实施例提供的差错交易标准化组件 102，通过 Java 通用接口技术实现，适用于各种操作系统，例如 Windows、Linux、Unix 等；以及各种中间件产品，例如 Websphere、Weblogic、Jboss、Tomcat 等。此外，通过配置参数来适应各银联成员机构 101 的机构代码、用户权限、文件路径等系统环境，从而满足各种技术条件下的银联成员机构 101 接入银联差错交易网络 103 的需求。

本发明实施例提供的差错交易标准化组件 102 包括：报文转换模块 1021，软件加密机 1022，签名模块 1023，证书管理模块 1024，证书库 1025，凭证文件编码解码模块 1026，安全通讯模块 1027。

报文转换模块 1021，用于将银联成员机构 101 的客户端发送的差错业务数据转换成标准格式的差错请求报文。

软件加密机 1022, 用于对差错请求报文中的敏感数据域进行加密, 保证报文的保密性。

签名模块 1023, 用于对差错请求报文中的关键字段进行签名, 保证报文的不可否认性和防篡改性。

证书管理模块 1024, 用于管理差错对接的安全认证证书。

证书库 1025 存储了 CFCA (China Financial Certification Authority, 中国金融认证中心) 签发给银联的非对称加密证书, 包括开发阶段、入网测试阶段和生产运行阶段的服务器端公钥、客户端私钥, 供证书管理模块 1024 使用。

凭证文件编码解码模块 1026, 用于对差错凭证文件进行编码和解码。

安全通讯模块 1027, 用于与银联差错交易网络建立双向认证的安全链接。

本发明实施例提供了接入银联差错交易网络对接客户端的统一接口, 各银联成员机构 101 只需调用本发明实施例提供的差错交易标准化组件 102, 即可实现与银联差错交易网络 103 的对接。银联成员机构 101 只需关注行内差错业务相关的处理和实现, 大大缩短了银联成员机构 101 的开发周期, 节省了开发、测试及运维成本, 提高了开发效率和运行稳定性。

本发明实施例提供一种差错交易的标准化方法, 如图 2 所示, 为本发明实施例提供的一种差错交易的标准化方流程图示意图, 包括:

步骤 201: 接收客户端发送的差错业务调用请求, 将差错业务调用请求转换为标准格式的交换报文。

其中, 客户端表示银联各成员机构的差错交易处理客户端平台。为了适配各个成员机构的差错交易处理客户端平台, 转换前的请求是一般的程序函数调用形式, 报文元素作为函数调用参数输入。例如:

```
SetReqMsgHeader ( getMsgHeader ( ));  
SetExpTransAt ( TransAtr );  
SetPriAccountNumber ( "6288888888888888" );  
SetSettleDt ( "20150101" );  
SetTransAmount ( TransAtr );
```

SetTransKey (“01033910 7537601215165420001030000”);

SetTransLogCd (“01”);

SetRequestSeqNumber (“123456789”);

具体地，可以通过报文转换模块 1021 实现本步骤的功能，标准格式的交换报文包括 XML (Extensible Markup Language, 可扩展标记语言) 报文标签名称和 XML 报文标签值。报文转换模块 1021 模块接收到调用后，根据预设的调用方法名称与报文标签的对应关系，将差错业务调用请求的调用方法名称转化成 XML 报文标签名称；然后根据将差错业务调用请求的调用方法名称对应的调用方法参数，将差错业务调用请求的调用方法参数转化成 XML 报文标签的值。转换后的交换报文符合银联差错对接联网联合规范的 XML 报文格式，可以被银联差错交易网络接收并按照交换报文中表示的差错业务含义进行处理。例如：

```
< data: SetRequestSeqNumber >123456789< /data: SetRequestSeqNumber >
< data: PriAccountNumber >6288888888888888</data: PriAccountNumber >
< data: SettleDt >20150101</data: SettleDt >
< data: TransAmount>10000</data: TransAmount>
< data: TransKey>01033910    7537601215165420001030000</data:
TransKey>
< data: TransLogCd>01</data: TransLogCd>
< data: ExpTransAt>10000</data: ExpTransAt>
```

步骤 202: 根据预设的证书库，对交换报文中的敏感数据域进行加密，生成加密报文域；以及对交换报文中的关键字段进行签名，生成签名报文域。

具体地，在上述的差错交易的标准化系统中，证书库 1025 存储了 CFCA 签发给银联的非对称加密证书，包括开发阶段、入网测试阶段和生产运行阶段的服务器公钥、客户端私钥。然而，银联差错交易网络接入的证书指定为 CFCA 的非对称加密证书，该证书从无法直接区分证书包含的密钥类型，如服务器公钥和/或客户端私钥；也无法区分证书类型，如入网联调测试证书和生

产证书。该特性给机构入网过程造成了很大困难。

本发明实施例通过证书管理模块 1024 对证书库 1025 进行管理，将证书库中单一标准格式的 CFCA 的非对称加密证书进行配置、读取和转化，提取出 CFCA 的非对称加密证书中的服务器公钥和客户端私钥，并转化为可读取调用的形式。提取后的服务器公钥和客户端私钥用于为签名、加密、安全通讯等各功能模块提供证书。例如，客户端私钥证书源格式为 pfx，服务器端公钥证书源格式为 crt，提取转换后的目的格式为 keystore、加密函数、签名函数等可以直接被调用的格式。

此外，证书管理模块 1024 将差错入网联调测试证书和生产证书进行区分，避免了证书使用中的混淆，保证在入网接入的不同阶段使用不同类型证书，大大提高了证书的管理性和使用效率。

进一步地，软件加密机 1022 从证书管理模块 1024 中调用服务器公钥，对差错业务调用请求的敏感数据域进行加密，生成加密报文域。敏感数据域包括密码等需要加密的敏感数据。加密后的信息只能被银联差错网络的服务器私钥进行解密，即使被非法截获也无法获取报文中的真实敏感信息，从而实现敏感信息的安全传输。

进一步地，签名模块 1023 从证书管理模块 1024 中调用客户端私钥，对差错业务调用请求中的关键字段进行签名，生成签名报文域。关键字段包括交易卡号、交易时间、交易金额等关键信息。签名后的信息被银联差错网络读取后，通过客户端公钥验证签名，验证通过确认合法后才对关键信息进行处理，实现了关键信息的不可否认性和防篡改性。

进一步地，若差错业务调用请求中包括二进制编码形式的凭证文件，则对凭证文件进行解码；并通过所述银联差错交易网络的编码方式（base64 编码方式）对所解码后的凭证文件进行编码，实现文件的安全传输。

步骤 203: 通过双向认证的安全通讯链路将包含加密报文域和签名报文域的交换报文发送至银联差错交易网络。

具体地，可以通过安全通讯模块 1027 实现本步骤的功能。其中，安全通

讯链路是在各银联成员机构的客户端与银联差错交易网络服务器之间建立的一条安全通讯链路。安全通讯模块 1027 从证书管理模块 1024 中调用服务器端公钥和客户端私钥，根据 HTTPS（Hyper Text Transfer Protocol over Secure Socket Layer，安全套接层上的超文本传输协议），与银联差错交易网络服务器间建立双向认证 SSL(Secure Sockets Layer，安全套接层)机制。双方安全认证通过后，将报文发送给银联差错交易网络服务器，并接收该服务端应答。

本发明实施例提供一种差错交易的标准化方法，将银联成员机构内部的客户端平台发送的差错业务调用请求转换为标准格式的交换报文，通过软件加密机对敏感数据域进行加密，通过签名模块对关键字段进行签名，通过凭证文件编码解码模块对凭证文件进行编码，将差错业务调用请求转换为银联差错交易网络可处理的、符合银联差错交易网络技术规范的报文。此外，通过 Java 通用接口技术实现各模块功能，灵活适配接入银联差错交易网络的各成员机构客户端系统，提供了通用、安全、便捷的客户端接入接口，缩短了成员机构的开发周期，降低了成员机构在测试、投产阶段的出错概率，大大降低了机构接入银联差错交易网络的成本。

基于同样的发明构思，本发明实施例还提供一种差错交易的标准化装置，如图 3 所示，为本发明实施例提供的一种差错交易的标准化装置结构示意图，包括：

格式转换单元 301：用于接收客户端发送的差错业务调用请求，将所述差错业务调用请求转换为标准格式的交换报文；

报文域转换单元 302：用于根据预设的证书库，对所述交换报文中的敏感数据域进行加密，生成加密报文域；以及对所述交换报文中的关键字段进行签名，生成签名报文域；

发送单元 303：用于通过双向认证的安全通讯链路将包含所述加密报文域和所述签名报文域的交换报文发送至银联差错交易网络。

较佳地，所述标准格式的交换报文包括可扩展标记语言 XML 报文标签名称和 XML 报文标签值，所述格式转换单元 301，具体用于：

根据预设的调用方法名称与报文标签的对应关系，将所述差错业务调用请求的调用方法名称转化成 XML 报文标签名称；

将所述差错业务调用请求的调用方法参数转化成 XML 报文标签的值。

较佳地，所述预设的证书库通过以下方式确定：

提取中国金融认证中心 CFCA 的非对称加密证书中的服务器公钥和客户端私钥，通过所述服务器公钥和客户端私钥确定所述预设证书库，所述 CFCA 的非对称加密证书用于接入银联差错交易网络。

较佳地，所述报文域转换单元 302，具体用于：

调用所述预设证书库中的服务器公钥，对所述差错业务调用请求的敏感数据域进行加密，生成加密报文域。

较佳地，所述报文域转换单元 302，具体用于：

调用所述预设证书库中的客户端私钥，对所述差错业务调用请求中的关键字段进行签名，生成签名报文域。

较佳地，所述双向认证的安全通讯链路通过以下方式确定：

调用所述预设证书库中的服务器公钥和客户端私钥，根据安全套接层上的超文本传输协议 HTTPS，建立与所述银联差错交易网络的双向认证的安全通讯链路。

较佳地，所述报文域转换单元 302，还用于：

若所述差错业务调用请求中包括二进制编码形式的凭证文件，则对所述凭证文件进行解码；

通过所述银联差错交易网络的编码方式对所解码后的凭证文件进行编码。

具体地，本发明实施例中的格式转换单元 301 的功能可通过本发明实施例提供的差错交易的标准化系统中的差错交易标准化组件 102 中的报文转换模块 1021 来实现。报文域转换单元 302 的功能可通过本发明实施例提供的差错交易的标准化系统中的差错交易标准化组件 102 中的软件加密机 1022、签名模块 1023、证书管理模块 1024、证书库 1025、凭证文件编码解码模块 1026

来实现。发送单元 303 的功能可通过本发明实施例提供的差错交易的标准化系统中的差错交易标准化组件 102 中的证书管理模块 1024、证书库 1025、安全通讯模块 1027 来实现。

本发明实施例提供一种差错交易的标准化装置，将银联成员机构内部的客户端平台发送的差错业务调用请求转换为标准格式的交换报文，通过软件加密机对敏感数据域进行加密，通过签名模块对关键字段进行签名，通过凭证文件编码解码模块对凭证文件进行编码，将差错业务调用请求转换为银联差错交易网络可处理的、符合银联差错交易网络技术规范 of 的报文。此外，通过 Java 通用接口技术实现各模块功能，灵活适配接入银联差错交易网络的各成员机构客户端系统，提供了通用、安全、便捷的客户端接入接口，缩短了成员机构的开发周期，降低了成员机构在测试、投产阶段的出错概率，大大降低了机构接入银联差错交易网络的成本。

基于相同的原理，本发明还提供一种电子设备，如图 4 所示，包括处理器 401、存储器 402、收发机 403、总线接口 404，其中处理器 401、存储器 402 与收发机 403 之间通过总线接口 404 连接；

所述收发机 403，用于接收客户端发送的差错业务调用请求；

所述处理器 401，用于将所述差错业务调用请求转换为标准格式的交换报文；根据预设的证书库，对所述交换报文中的敏感数据域进行加密，生成加密报文域；以及对所述交换报文中的关键字段进行签名，生成签名报文域；通过双向认证的安全通讯链路将包含所述加密报文域和所述签名报文域的交换报文发送至银联差错交易网络；

所述存储器 402，用于存储一个或多个可执行程序，可以存储所述处理器在执行操作时所使用的数据；

所述总线接口 404，用于提供接口。

进一步地，所述标准格式的交换报文包括可扩展标记语言 XML 报文标签名称和 XML 报文标签值，所述处理器 401 将所述差错业务调用请求转换为标准格式的交换报文，具体用于：

根据预设的调用方法名称与报文标签的对应关系，将所述差错业务调用请求的调用方法名称转化成 XML 报文标签名称；

将所述差错业务调用请求的调用方法参数转化成 XML 报文标签的值。

进一步地，所述预设的证书库通过以下方式确定：

提取中国金融认证中心 CFCA 的非对称加密证书中的服务器公钥和客户端私钥，通过所述服务器公钥和客户端私钥确定所述预设证书库，所述 CFCA 的非对称加密证书用于接入银联差错交易网络。

进一步地，所述处理器 401 根据预设的证书库，对所述差错业务调用请求的敏感数据域进行加密，生成加密报文域，具体用于：

调用所述预设证书库中的服务器公钥，对所述差错业务调用请求的敏感数据域进行加密，生成加密报文域。

进一步地，所述差错业务调用请求中的关键字段进行签名，所述处理器 401 生成签名报文域，具体用于：

调用所述预设证书库中的客户端私钥，对所述差错业务调用请求中的关键字段进行签名，生成签名报文域。

进一步地，所述双向认证的安全通讯链路通过以下方式确定：

调用所述预设证书库中的服务器公钥和客户端私钥，根据安全套接层上的超文本传输协议 HTTPS，建立与所述银联差错交易网络的双向认证的安全通讯链路。

进一步地，所述处理器 401 通过安全通讯链路将包含所述加密报文域和所述签名报文域的所述交换报文发送至银联差错交易网络之前，还用于：

若所述差错业务调用请求中包括二进制编码形式的凭证文件，则对所述凭证文件进行解码；

通过所述银联差错交易网络的编码方式对所解码后的凭证文件进行编码。

本申请实施例提供了一种非暂态计算机可读存储介质，所述非暂态计算机可读存储介质存储计算机指令，所述计算机指令用于使所述计算机执行任

——项差错交易的标准化方法。

本申请实施例提供了一种计算机程序产品，所述计算机程序产品包括存储在非暂态计算机可读存储介质上的计算程序，所述计算机程序包括程序指令，当所述程序指令被计算机执行时，使所述计算机执行上述任一项差错交易的标准化方法。

本领域内的技术人员应明白，本发明的实施例可提供为方法、系统、或计算机程序产品。因此，本发明可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本发明可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质（包括但不限于磁盘存储器、CD-ROM、光学存储器等）上实施的计算机程序产品的形式。

本发明是参照根据本发明实施例的方法、设备（系统）、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器，使得通过该计算机或其他可编程数据处理设备的处理器执行的指令可实现流程图中的一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图的一个流程或多个流程和/或方框图的一个方框或多个方框中指定的功能的步骤。

尽管已描述了本发明的优选实施例，但本领域内的技术人员一旦得知了

基本创造性概念，则可对这些实施例作出另外的变更和修改。所以，所附权利要求意欲解释为包括优选实施例以及落入本发明范围的所有变更和修改。

显然，本领域的技术人员可以对本发明进行各种改动和变型而不脱离本发明的精神和范围。这样，倘若本发明的这些修改和变型属于本发明权利要求及其等同技术的范围之内，则本发明也意图包含这些改动和变型在内。

权 利 要 求

1、一种差错交易的标准化方法，其特征在于，包括：

接收客户端发送的差错业务调用请求，将所述差错业务调用请求转换为标准格式的交换报文；

根据预设的证书库，对所述交换报文中的敏感数据域进行加密，生成加密报文域；以及对所述交换报文中的关键字段进行签名，生成签名报文域；

通过双向认证的安全通讯链路将包含所述加密报文域和所述签名报文域的交换报文发送至银联差错交易网络。

2、如权利要求 1 所述的方法，其特征在于，所述标准格式的交换报文包括可扩展标记语言 XML 报文标签名称和 XML 报文标签值，所述将所述差错业务调用请求转换为标准格式的交换报文，包括：

根据预设的调用方法名称与报文标签的对应关系，将所述差错业务调用请求的调用方法名称转化成 XML 报文标签名称；

将所述差错业务调用请求的调用方法参数转化成 XML 报文标签的值。

3、如权利要求 1 所述的方法，其特征在于，所述预设的证书库通过以下方式确定：

提取中国金融认证中心 CFCA 的非对称加密证书中的服务器公钥和客户端私钥，通过所述服务器公钥和客户端私钥确定所述预设证书库，所述 CFCA 的非对称加密证书用于接入银联差错交易网络。

4、如权利要求 3 所述的方法，其特征在于，所述根据预设的证书库，对所述差错业务调用请求的敏感数据域进行加密，生成加密报文域，包括：

调用所述预设证书库中的服务器公钥，对所述差错业务调用请求的敏感数据域进行加密，生成加密报文域。

5、如权利要求 3 所述的方法，其特征在于，所述差错业务调用请求中的关键字段进行签名，生成签名报文域，包括：

调用所述预设证书库中的客户端私钥，对所述差错业务调用请求中的关

键字段进行签名，生成签名报文域。

6、如权利要求 3 所述的方法，其特征在于，所述双向认证的安全通讯链路通过以下方式确定：

调用所述预设证书库中的服务器公钥和客户端私钥，根据安全套接层上的超文本传输协议 HTTPS，建立与所述银联差错交易网络的双向认证的安全通讯链路。

7、如权利要求 1~6 任一项所述的方法，其特征在于，所述通过安全通讯链路将包含所述加密报文域和所述签名报文域的所述交换报文发送至银联差错交易网络之前，还包括：

若所述差错业务调用请求中包括二进制编码形式的凭证文件，则对所述凭证文件进行解码；

通过所述银联差错交易网络的编码方式对所解码后的凭证文件进行编码。

8、一种差错交易的标准化装置，其特征在于，包括：

格式转换单元：用于接收客户端发送的差错业务调用请求，将所述差错业务调用请求转换为标准格式的交换报文；

报文域转换单元：用于根据预设的证书库，对所述交换报文中的敏感数据域进行加密，生成加密报文域；以及对所述交换报文中的关键字段进行签名，生成签名报文域；

发送单元：用于通过双向认证的安全通讯链路将包含所述加密报文域和所述签名报文域的交换报文发送至银联差错交易网络。

9、如权利要求 8 所述的装置，其特征在于，所述标准格式的交换报文包括可扩展标记语言 XML 报文标签名称和 XML 报文标签值，所述格式转换单元，具体用于：

根据预设的调用方法名称与报文标签的对应关系，将所述差错业务调用请求的调用方法名称转化成 XML 报文标签名称；

将所述差错业务调用请求的调用方法参数转化成 XML 报文标签的值。

10、如权利要求 8 所述的装置，其特征在于，所述预设的证书库通过以下方式确定：

提取中国金融认证中心 CFCA 的非对称加密证书中的服务器公钥和客户端私钥，通过所述服务器公钥和客户端私钥确定所述预设证书库，所述 CFCA 的非对称加密证书用于接入银联差错交易网络。

11、如权利要求 10 所述的装置，其特征在于，所述报文域转换单元，具体用于：

调用所述预设证书库中的服务器公钥，对所述差错业务调用请求的敏感数据域进行加密，生成加密报文域。

12、如权利要求 10 所述的装置，其特征在于，所述报文域转换单元，具体用于：

调用所述预设证书库中的客户端私钥，对所述差错业务调用请求中的关键字段进行签名，生成签名报文域。

13、如权利要求 10 所述的装置，其特征在于，所述双向认证的安全通讯链路通过以下方式确定：

调用所述预设证书库中的服务器公钥和客户端私钥，根据安全套接层上的超文本传输协议 HTTPS，建立与所述银联差错交易网络的双向认证的安全通讯链路。

14、如权利要求 8~13 任一项所述的装置，其特征在于，所述报文域转换单元，还用于：

若所述差错业务调用请求中包括二进制编码形式的凭证文件，则对所述凭证文件进行解码；

通过所述银联差错交易网络的编码方式对所解码后的凭证文件进行编码。

15、一种电子设备，其特征在于，包括处理器、存储器、收发机、总线接口，其中处理器、存储器与收发机之间通过总线接口连接；

所述收发机，用于接收客户端发送的差错业务调用请求；

所述处理器，

用于将所述差错业务调用请求转换为标准格式的交换报文；根据预设的证书库，对所述交换报文中的敏感数据域进行加密，生成加密报文域；以及对所述交换报文中的关键字段进行签名，生成签名报文域；通过双向认证的安全通讯链路将包含所述加密报文域和所述签名报文域的交换报文发送至银联差错交易网络；

所述存储器，用于存储一个或多个可执行程序，可以存储所述处理器在执行操作时所使用的数据；

所述总线接口，用于提供接口。

16、如权利要求 15 所述的设备，其特征在于，所述标准格式的交换报文包括可扩展标记语言 XML 报文标签名称和 XML 报文标签值，所述处理器将所述差错业务调用请求转换为标准格式的交换报文，具体用于：

根据预设的调用方法名称与报文标签的对应关系，将所述差错业务调用请求的调用方法名称转化成 XML 报文标签名称；

将所述差错业务调用请求的调用方法参数转化成 XML 报文标签的值。

17、如权利要求 15 所述的设备，其特征在于，所述预设的证书库通过以下方式确定：

提取中国金融认证中心 CFCA 的非对称加密证书中的服务器公钥和客户端私钥，通过所述服务器公钥和客户端私钥确定所述预设证书库，所述 CFCA 的非对称加密证书用于接入银联差错交易网络。

18、如权利要求 17 所述的设备，其特征在于，所述处理器根据预设的证书库，对所述差错业务调用请求的敏感数据域进行加密，生成加密报文域，具体用于：

调用所述预设证书库中的服务器公钥，对所述差错业务调用请求的敏感数据域进行加密，生成加密报文域。

19、如权利要求 17 所述的设备，其特征在于，所述差错业务调用请求中的关键字段进行签名，所述处理器生成签名报文域，具体用于：

调用所述预设证书库中的客户端私钥，对所述差错业务调用请求中的关键字段进行签名，生成签名报文域。

20、如权利要求 17 所述的设备，其特征在于，所述双向认证的安全通讯链路通过以下方式确定：

调用所述预设证书库中的服务器公钥和客户端私钥，根据安全套接层上的超文本传输协议 HTTPS，建立与所述银联差错交易网络的双向认证的安全通讯链路。

21、如权利要求 15~20 任一所述的设备，其特征在于，所述处理器通过安全通讯链路将包含所述加密报文域和所述签名报文域的所述交换报文发送至银联差错交易网络之前，还用于：

若所述差错业务调用请求中包括二进制编码形式的凭证文件，则对所述凭证文件进行解码；

通过所述银联差错交易网络的编码方式对所解码后的凭证文件进行编码。

22、一种非暂态计算机可读存储介质，其特征在于，所述非暂态计算机可读存储介质存储计算机指令，所述计算机指令用于使所述计算机执行权利要求 1~7 任一所述方法。

23、一种计算机程序产品，其特征在于，所述计算机程序产品包括存储在非暂态计算机可读存储介质上的计算程序，所述计算机程序包括程序指令，当所述程序指令被计算机执行时，使所述计算机执行权利要求 1~7 任一所述方法。

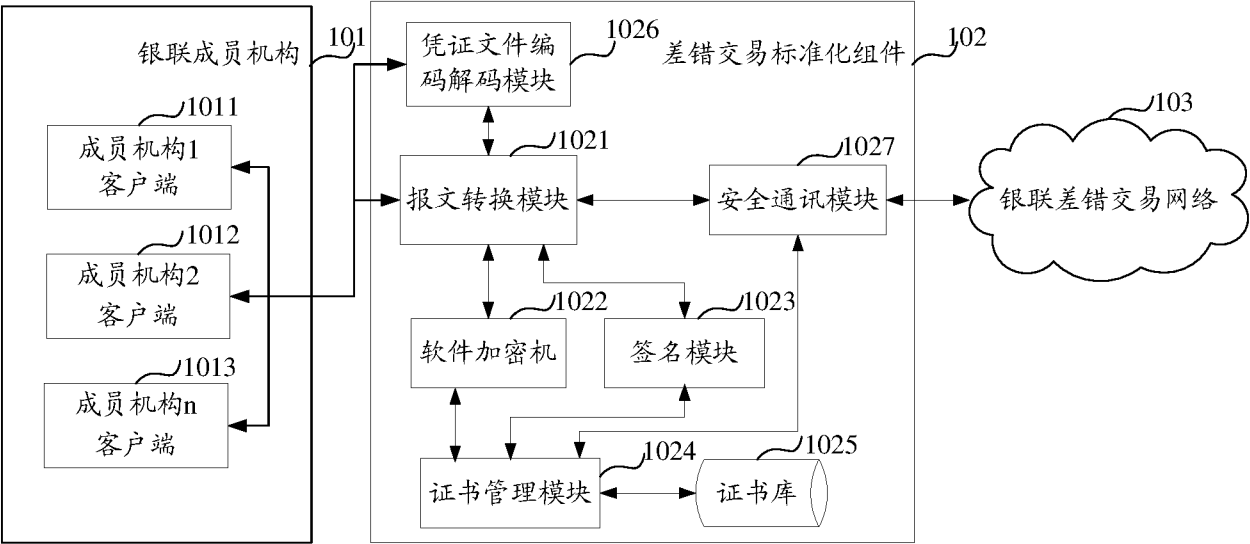


图 1

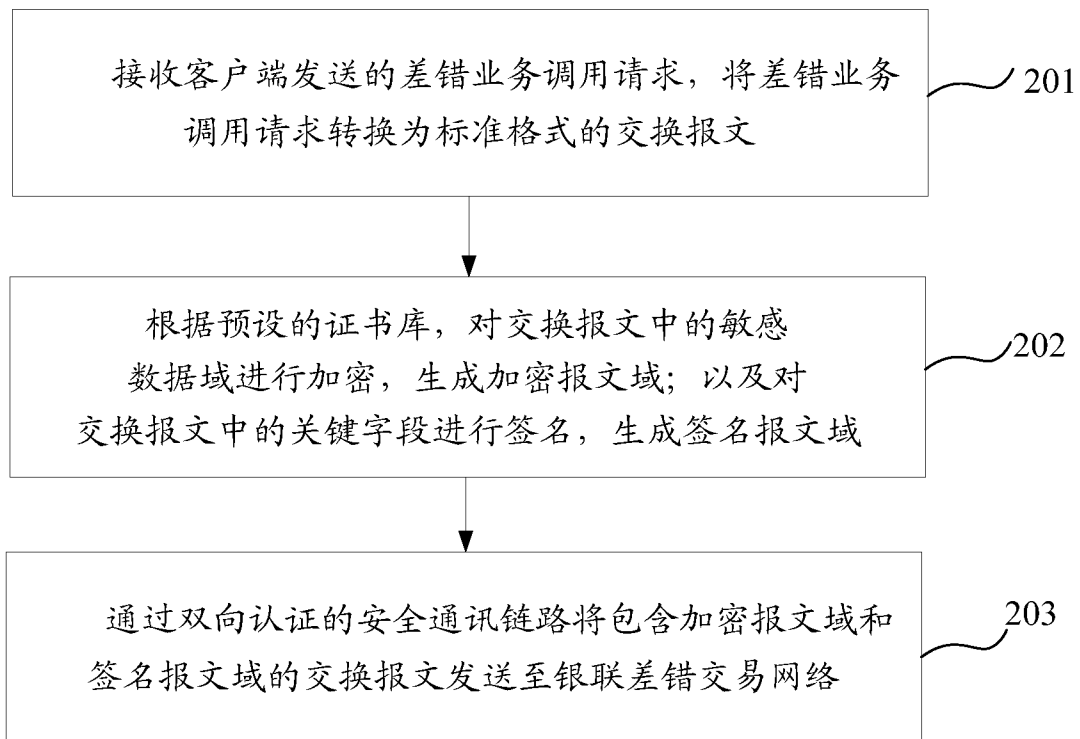


图 2



图 3

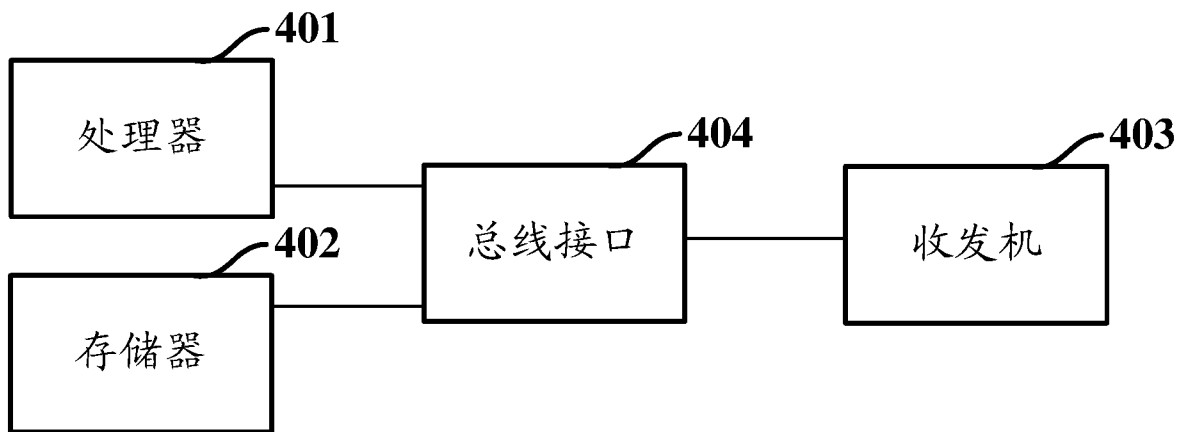


图 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2017/107454

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/08 (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)

H04L

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)

CPRSABS, CNTXT, CNKI, VEN, DWPI, USTXT: 差错, 网络, 平台, 加密, 签名, 证书, 请求, xml, 标准, 格式, 支付, error, network, platform, encrypt+, signature, certificate, request, standard, format, pay

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 106603636 A (CHINA UNIONPAY CO., LTD.), 26 April 2017 (26.04.2017), claims 1-14, and description, paragraphs [0001]-[0114]	1-23
X	CN 1681260 A (CHINA UNIONPAY CO., LTD.), 12 October 2005 (12.10.2005), description, page 1, line 5 to page 6, line 25, page 11, lines 15-20, and page 13, lines 2-10	1-2, 8-9, 15-16, 22-23
Y	CN 1681260 A (CHINA UNIONPAY CO., LTD.), 12 October 2005 (12.10.2005), description, page 1, line 5 to page 6, line 25, page 11, lines 15-20, and page 13, lines 2-10	3-7, 10-14, 17-21
Y	CN 201570063 U (BEIJING RURAL COMMERCIAL BANK CO., LTD.), 01 September 2010 (01.09.2010), description, paragraphs [0026]-[0028]	3-7, 10-14, 17-21
X	US 2009154699 A1 (VERIZON SERVICES ORGANIZATION INC.), 18 June 2009 (18.06.2009), description, paragraphs [0016]-[0030] and [0063]-[0073]	1-2, 8-9, 15-16, 22-23

☐ 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 01 January 2018	Date of mailing of the international search report 29 January 2018
--	---

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 LI, Xiaoqian Telephone No. (86-10) 62089456
---	--

International application No.
PCT/CN2017/107454

Form PCT/ISA/210 (patent family annex) (July 2009)

国际检索报告

国际申请号

PCT/CN2017/107454

A. 主题的分类

H04L 29/08(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)

H04L

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))

CPRSABS, CNTXT, CNKI, VEN, DWPI, USTXT: 差错, 网络, 平台, 加密, 签名, 证书, 请求, xml, 标准, 格式, 支付, error, network, platform, encrypt+, signature, certificate, request, standard, format, pay

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
PX	CN 106603636 A (中国银联股份有限公司) 2017年 4月 26日 (2017 - 04 - 26) 权利要求1-14, 说明书第[0001]-[0114]段	1-23
X	CN 1681260 A (中国银行股份有限公司) 2005年 10月 12日 (2005 - 10 - 12) 说明书第1页第5行至第6页第25行, 第11页第15-20行, 第13页第2-10行	1-2, 8-9, 15-16, 22-23
Y	CN 1681260 A (中国银行股份有限公司) 2005年 10月 12日 (2005 - 10 - 12) 说明书第1页第5行至第6页第25行, 第11页第15-20行, 第13页第2-10行	3-7, 10-14, 17-21
Y	CN 201570063 U (北京农村商业银行股份有限公司) 2010年 9月 1日 (2010 - 09 - 01) 说明书第[0026]-[0028]段	3-7, 10-14, 17-21
X	US 2009154699 A1 (VERIZON SERVICES ORGANIZATION INC.) 2009年 6月 18日 (2009 - 06 - 18) 说明书第[0016]-[0030]段, [0063]-[0073]段	1-2, 8-9, 15-16, 22-23

☐ 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

2018年 1月 1日

国际检索报告邮寄日期

2018年 1月 29日

ISA/CN的名称和邮寄地址

中华人民共和国国家知识产权局(ISA/CN)
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

李晓茜

电话号码 (86-10) 62089456

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2017/107454

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	106603636	A	2017年 4月 26日	无			
CN	1681260	A	2005年 10月 12日	CN	100448215	C	2008年 12月 31日
CN	201570063	U	2010年 9月 1日	无			
US	2009154699	A1	2009年 6月 18日	无			