[19] Patents Registry
The Hong Kong Special Administrative Region
香港特別行政區
專利註冊處

[11] 1237145 B
CN 106603636 B

[12] **STANDARD PATENT (R) SPECIFICATION**
轉錄標準專利說明書

[21] Application no. 申請編號
17110770.6

[22] Date of filing 提交日期
23.10.2017

[51] Int. Cl.
H04L 29/08 (2006.01) G06Q 40/02 (2012.01)

[54] ERROR TRANSACTION STANDARDIZATION METHOD AND DEVICE
一種差錯交易的標準化方法及裝置

[43] Date of publication of application 申請發表日期
06.04.2018

[45] Date of publication of grant of patent 批予專利的發表日期
15.01.2021

CN Application no. & date 中國專利申請編號及日期
CN 201611076397.8 29.11.2016

CN Publication no. & date 中國專利申請發表編號及日期
CN 106603636 26.04.2017

Date of grant in designated patent office 指定專利當局批予專利日期
26.05.2020

[73] Proprietor 專利所有人
CHINA UNIONPAY CO., LTD.
中国银联股份有限公司
CUP Tower, 36 Hanxiao Road
Pudong New Area Shanghai 200135
CHINA

[72] Inventor 發明人
GUO, Hongqiang 郭弘强
LI, Wei 李伟
TANG, Zhen 唐真

[74] Agent and / or address for service 代理人及/或送達地址
BARRON & YOUNG INTELLECTUAL PROPERTY LIMITED
Suite 617, Lakeside 2
No. 10 Science Park West Avenue, Hong Kong Science Park, Shatin, N.T.
HONG KONG

(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 106603636 B
(45)授权公告日 2020.05.26

(21)申请号 201611076397.8
(22)申请日 2016.11.29
(65)同一申请的已公布的文献号
申请公布号 CN 106603636 A
(43)申请公布日 2017.04.26
(73)专利权人 中国银联股份有限公司
地址 200135 上海市浦东新区含笑路36号
(72)发明人 郭弘强 李伟 唐真
(74)专利代理机构 北京同达信恒知识产权代理有限公司 11291
代理人 黄志华
(51)Int.Cl.
H04L 29/08(2006.01)
G06Q 40/02(2012.01)

审查员 许顺频

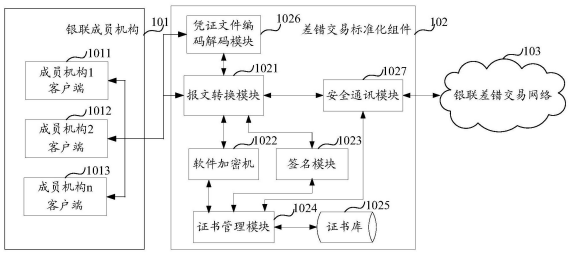
权利要求书2页 说明书8页 附图2页

(54)发明名称

一种差错交易的标准化方法及装置

(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。



CN 106603636 B

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;

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;

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;以及根据所述预设的证书库,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。

4.如权利要求1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。

5.如权利要求1～4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。

6.一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;还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;以及根据所述预设的证书库,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。

7.如权利要求6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。

8.如权利要求6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。

9.如权利要求6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。

10.如权利要求6～9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。

一种差错交易的标准化方法及装置

技术领域

[0001] 本发明涉及互联网领域，尤其涉及一种差错交易网络的标准化方法及装置。

背景技术

[0002] 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。

[0003] 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。

[0004] 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。

[0005] 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

[0006] 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。

[0007] 本发明实施例提供一种差错交易的标准化方法，包括：

[0008] 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；

[0009] 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；

[0010] 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。

[0011] 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：

[0012] 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；

[0013] 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。

[0014] 较佳地，所述预设的证书库通过以下方式确定：

[0015] 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。

[0016] 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：

[0017] 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。

[0018] 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：

[0019] 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。

[0020] 较佳地，所述双向认证的安全通讯链路通过以下方式确定：

[0021] 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。

[0022] 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：

[0023] 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；

[0024] 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。

[0025] 本发明实施例还提供一种差错交易的标准化装置，包括：

[0026] 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；

[0027] 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；

[0028] 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。

[0029] 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：

[0030] 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；

[0031] 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。

[0032] 较佳地，所述预设的证书库通过以下方式确定：

[0033] 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。

[0034] 较佳地，所述报文域转换单元，具体用于：

[0035] 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。

[0036] 较佳地，所述报文域转换单元，具体用于：

[0037] 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。

[0038] 较佳地,所述双向认证的安全通讯链路通过以下方式确定:

[0039] 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。

[0040] 较佳地,所述报文域转换单元,还用于:

[0041] 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;

[0042] 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。

[0043] 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

[0044] 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。

[0045] 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;

[0046] 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;

[0047] 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。

具体实施方式

[0048] 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。

[0049] 本发明实施例中中国银联是指中国银行卡联合组织,通过银联跨行交易清算系统,实现商业银行系统间的互联互通和资源共享,保证银行卡跨行、跨地区和跨境的使用。本发明实施例中的银联成员机构包括收单机构、银行卡联合组织、发卡机构等参与交易业务的成员机构。

[0050] 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。

[0051] 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。

[0052] 本发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。

[0053] 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。

[0054] 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。

[0055] 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。

[0056] 证书管理模块1024，用于管理差错对接的安全认证证书。

[0057] 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。

[0058] 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。

[0059] 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。

[0060] 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。

[0061] 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示意图，包括：

[0062] 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。

[0063] 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：

[0064] SetReqMsgHeader(getMsgHeader())；

[0065] SetExpTransAt(TransAtr)；

[0066] SetPriAccountNumber(“6288888888888888”)；

[0067] SetSettleDt(“20150101”)；

[0068] SetTransAmount(TransAtr)；

[0069] SetTransKey(“01033910 75376012151654200010300000”)；

[0070] SetTransLogCd(“01”)；

[0071] SetRequestSeqNumber(“123456789”)；

[0072] 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：

[0073] <data:SetRequestSeqNumber>123456789</data:SetRequestSeqNumber>

[0074] <data:PriAccountNumber>6288888888888888</data:PriAccountNumber>

[0075] <data:SettleDt>20150101</data:SettleDt>

[0076] <data:TransAmount>10000</data:TransAmount>

[0077] <data:TransKey>01033910 75376012151654200010300000</data:TransKey>

[0078] <data:TransLogCd>01</data:TransLogCd>

[0079] <data:ExpTransAt>10000</data:ExpTransAt>

[0080] 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。

[0081] 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。

[0082] 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。

[0083] 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。

[0084] 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。

[0085] 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。

[0086] 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。

[0087] 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。

[0088] 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。

[0089] 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。

[0090] 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：

[0091] 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；

[0092] 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；

[0093] 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。

[0094] 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：

[0095] 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；

[0096] 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。

[0097] 较佳地，所述预设的证书库通过以下方式确定：

[0098] 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。

[0099] 较佳地，所述报文域转换单元302，具体用于：

[0100] 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。

[0101] 较佳地，所述报文域转换单元302，具体用于：

[0102] 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。

[0103] 较佳地，所述双向认证的安全通讯链路通过以下方式确定：

[0104] 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。

[0105] 较佳地，所述报文域转换单元302，还用于：

[0106] 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；

[0107] 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。

[0108] 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。

[0109] 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。

[0110] 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以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于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的系统。

[0111] 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系统的制造品，该指令系统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。

[0112] 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的步骤。

[0113] 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。

[0114] 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。

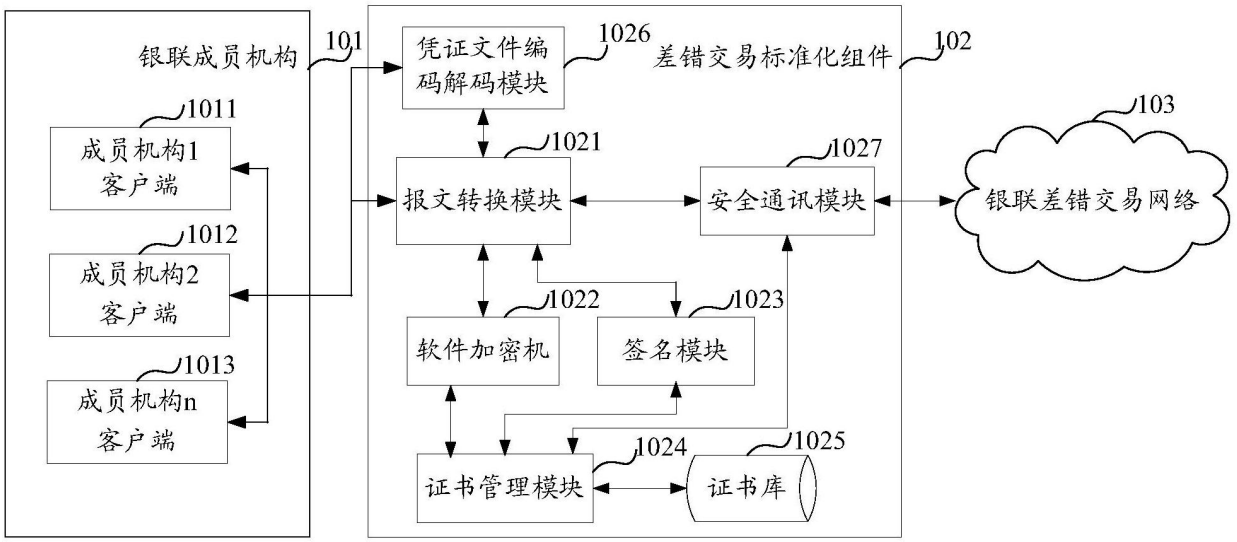

银联成员机构
101
成员机构1
客户端
1011
成员机构2
客户端
1012
成员机构n
客户端
1013
凭证文件编
码解码模块
1026
差错交易标准化组件
102
报文转换模块
1021
安全通讯模块
1027
103
银联差错交易网络
软件加密机
1022
签名模块
1023
证书管理模块
1024
证书库
1025

图1

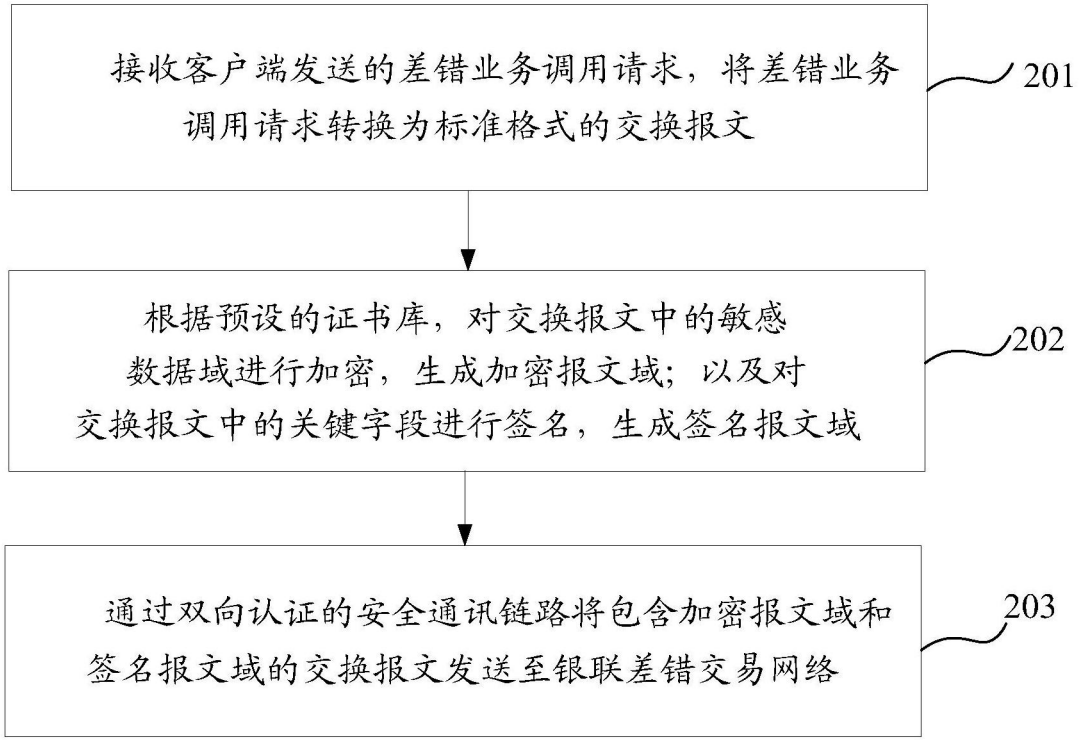

接收客户端发送的差错业务调用请求，将差错业务
调用请求转换为标准格式的交换报文
201
根据预设的证书库，对交换报文中的敏感
数据域进行加密，生成加密报文域；以及对
交换报文中的关键字段进行签名，生成签名报文域
202
通过双向认证的安全通讯链路将包含加密报文域和
签名报文域的交换报文发送至银联差错交易网络
203

图2

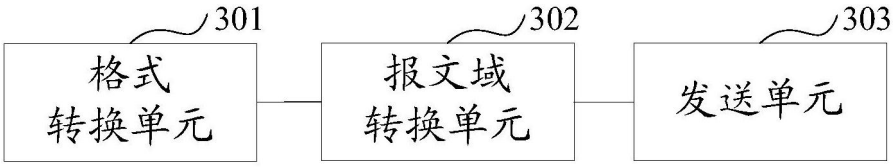


图3