



(12) 发明专利申请

(10) 申请公布号 CN 104486356 A

(43) 申请公布日 2015. 04. 01

(21) 申请号 201410842099. X

(22) 申请日 2014. 12. 29

(71) 申请人 芜湖乐锐思信息咨询有限公司

地址 241000 安徽省芜湖市镜湖区莲塘新村
瑞丰园 B 棟 07 号

(72) 发明人 高辉 赵迪

(51) Int. Cl.

H04L 29/06(2006. 01)

G06Q 20/38(2012. 01)

G06Q 20/16(2012. 01)

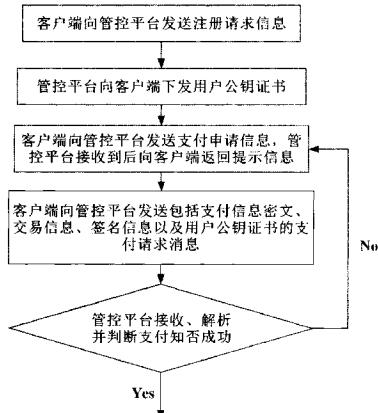
权利要求书1页 说明书2页 附图1页

(54) 发明名称

基于互联网在线交易的数据传输方法

(57) 摘要

本发明涉及网路通信技术领域，具体的说是一种特别适用于在线电子商务平台的保密性强、安全性好的基于互联网在线交易的数据传输方法，包括：客户端向管控平台发送注册请求信息，管控平台相应请求并要求提供认证请求信息，管控平台接收请求并客户端返回注册申请表，客户端接收用户注册信息，生成用户公私钥对，并储存公钥和私钥；客户端向管控平台发送加载有公钥证书和注册信息的注册申请表，管控中心接收请求并审核申请表的完整性，对于符合要求的申请表采用 CA 私钥对用户公钥进行签名，生成并存储用户公钥证书，向客户端下发用户公钥证书，本发明与现有技术相比，具有运算量小，成本低，安全可靠等显著的优点。



1. 一种基于互联网在线交易的数据传输方法,其特征在于包括以下步骤:

步骤 1 :客户端向管控平台发送注册请求信息,管控平台接收请求并客户端返回注册申请表,客户端接收用户注册信息,生成用户公私钥对,并储存公钥和私钥;

步骤 2 :客户端向管控平台发送加载有公钥证书和注册信息的注册申请表,管控中心接收请求并审核申请表的完整性,对于符合要求的申请表采用 CA 私钥对用户公钥进行签名,生成并存储用户公钥证书,向客户端下发用户公钥证书;

步骤 3 :客户端向管控平台发送支付申请信息,管控平台接收到后向客户端返回提示信息;

步骤 4 :客户端根据接收的提示信息输入支付信息和交易信息,使用数据加密密钥对所属支付信息加密处理获得支付信息密文,并对支付信息密文和交易信息进行哈希运算生成消息摘要,应用客户端的私钥对该消息摘要进行签名运算生成签名信息,客户端再次向管控平台发送包括支付信息密文、交易信息、签名信息以及用户公钥证书的支付请求消息;

步骤 5 :管控平台接收上述消息后,应用 CA 公钥对用户公钥证书进行解析获得用户公钥,应用用户公钥对接收的签名信息进行解析运算,形成消息摘要,应用与客户端约定的哈希函数对接收的支付信息密文和交易信息进行哈希运算,获得运算结果,将运算结果与消息摘要进行比较,若相同,则生成支付认证成功信息,支付认证成功,否则支付认证失败,向客户端返回支付失败信息。

2. 根据权利要求 1 所述的一种基于互联网在线交易的数据传输方法,其特征在于步骤 1 中管控平台接收客户端的注册请求信息后,对其进行备份存储。

3. 根据权利要求 1 所述的一种基于互联网在线交易的数据传输方法,其特征在于当支付认证成功后,管控平台应用数据加密密钥对支付信息密文进行解密处理,从而获得支付信息,并将支付信息中包含的支付账号以及密码与管控平台进行认证时存储的备份信息进行验证,若验证通过,则从支付信息所包含的支付账号中扣除相应支付金额,并将支付业务交易信息反馈给客户端,否则,向客户端返回支付失败信息。

4. 根据权利要求 3 所述的一种基于互联网在线交易的数据传输方法,其特征在于所述数据加密密钥是管控中心与客户端预先约定的。

基于互联网在线交易的数据传输方法

技术领域：

[0001] 本发明涉及网路通信技术领域，具体的说是一种特别适用于在线电子商务平台的保密性强、安全性好的基于互联网在线交易的数据传输方法。

背景技术：

[0002] 随着信息技术的发展和智能手机的普及，在网上完成商品交易已经成为现实，电子商务不仅给用户和企业带来了面对面的机会，优化了资源配置，而且节省了商铺费用。目前电子商务飞速发展，安全和诚信问题成为制约电子商务发展的关键环节。调查显示，有能力网购而不网购的消费者中，80%是出于信用及安全方面的担忧。由于不信任，目前大宗交易要在线下交易，成本高昂，如果有可信的服务提供商，未来中国互联网交易量还将持续增长。

发明内容：

[0003] 本发明针对现有技术中存在的缺点和不足，提出了一种特别适用于在线电子商务平台的保密性强、安全性好的基于互联网在线交易的数据传输方法。

[0004] 本发明可以通过以下措施达到：

[0005] 一种基于互联网在线交易的数据传输方法，其特征在于包括以下步骤：

[0006] 步骤 1：客户端向管控平台发送注册请求信息，管控平台接收请求并客户端返回注册申请表，客户端接收用户注册信息，生成用户公私钥对，并储存公钥和私钥；

[0007] 步骤 2：客户端向管控平台发送加载有公钥证书和注册信息的注册申请表，管控中心接收请求并审核申请表的完整性，对于符合要求的申请表采用 CA 私钥对用户公钥进行签名，生成并存储用户公钥证书，向客户端下发用户公钥证书；

[0008] 步骤 3：客户端向管控平台发送支付申请信息，管控平台接收到后向客户端返回提示信息；

[0009] 步骤 4：客户端根据接收的提示信息输入支付信息和交易信息，使用数据加密密钥对所属支付信息加密处理获得支付信息密文，并对支付信息密文和交易信息进行哈希运算生成消息摘要，应用客户端的私钥对该消息摘要进行签名运算生成签名信息，客户端再次向管控平台发送包括支付信息密文、交易信息、签名信息以及用户公钥证书的支付请求消息；

[0010] 步骤 5：管控平台接收上述消息后，应用 CA 公钥对用户公钥证书进行解析获得用户公钥，应用用户公钥对接收的签名信息进行解析运算，形成消息摘要，应用与客户端约定的哈希函数对接收的支付信息密文和交易信息进行哈希运算，获得运算结果，将运算结果与消息摘要进行比较，若相同，则生成支付认证成功信息，支付认证成功，否则支付认证失败，向客户端返回支付失败信息，或返回步骤 3 进行下一次支付。

[0011] 本发明步骤 1 中管控平台接收客户端的注册请求信息后，对其进行备份存储。

[0012] 本发明当支付认证成功后，管控平台应用数据加密密钥对支付信息密文进行解密

处理,从而获得支付信息,并将支付信息中包含的支付账号以及密码与管控平台进行认证时存储的备份信息进行验证,若验证通过,则从支付信息所包含的支付账号中扣除相应支付金额,并将支付业务交易信息反馈给客户端,否则,向客户端返回支付失败信息。

[0013] 本发明所述数据加密密钥是管控中心与客户端预先约定的。

[0014] 本发明与现有技术相比,具有运算量小,成本低,安全可靠等显著的优点。

附图说明 :

[0015] 附图 1 是本发明的流程图。

具体实施方式 :

[0016] 下面结合附图对本发明作进一步的说明。

[0017] 如图所示,本发明提出了一种基于互联网在线交易的数据传输方法,其特征在于包括以下步骤:

[0018] 步骤 1:客户端向管控平台发送注册请求信息,管控平台接收请求并客户端返回注册申请表,客户端接收用户注册信息,生成用户公私钥对,并储存公钥和私钥;

[0019] 步骤 2:客户端向管控平台发送加载有公钥证书和注册信息的注册申请表,管控中心接收请求并审核申请表的完整性,对于符合要求的申请表采用 CA 私钥对用户公钥进行签名,生成并存储用户公钥证书,向客户端下发用户公钥证书;

[0020] 步骤 3:客户端向管控平台发送支付申请信息,管控平台接收到后向客户端返回提示信息;

[0021] 步骤 4:客户端根据接收的提示信息输入支付信息和交易信息,使用数据加密密钥对所属支付信息加密处理获得支付信息密文,并对支付信息密文和交易信息进行哈希运算生成消息摘要,应用客户端的私钥对该消息摘要进行签名运算生成签名信息,客户端再次向管控平台发送包括支付信息密文、交易信息、签名信息以及用户公钥证书的支付请求消息;

[0022] 步骤 5:管控平台接收上述消息后,应用 CA 公钥对用户公钥证书进行解析获得用户公钥,应用用户公钥对接收的签名信息进行解析运算,形成消息摘要,应用与客户端约定的哈希函数对接收的支付信息密文和交易信息进行哈希运算,获得运算结果,将运算结果与消息摘要进行比较,若相同,则生成支付认证成功信息,支付认证成功,否则支付认证失败,向客户端返回支付失败信息。

[0023] 本发明步骤 1 中管控平台接收客户端的注册请求信息后,对其进行备份存储。

[0024] 本发明当支付认证成功后,管控平台应用数据加密密钥对支付信息密文进行解密处理,从而获得支付信息,并将支付信息中包含的支付账号以及密码与管控平台进行认证时存储的备份信息进行验证,若验证通过,则从支付信息所包含的支付账号中扣除相应支付金额,并将支付业务交易信息反馈给客户端,否则,向客户端返回支付失败信息。

[0025] 本发明所述数据加密密钥是管控中心与客户端预先约定的。

[0026] 本发明与现有技术相比,具有运算量小,成本低,安全可靠等显著的优点。

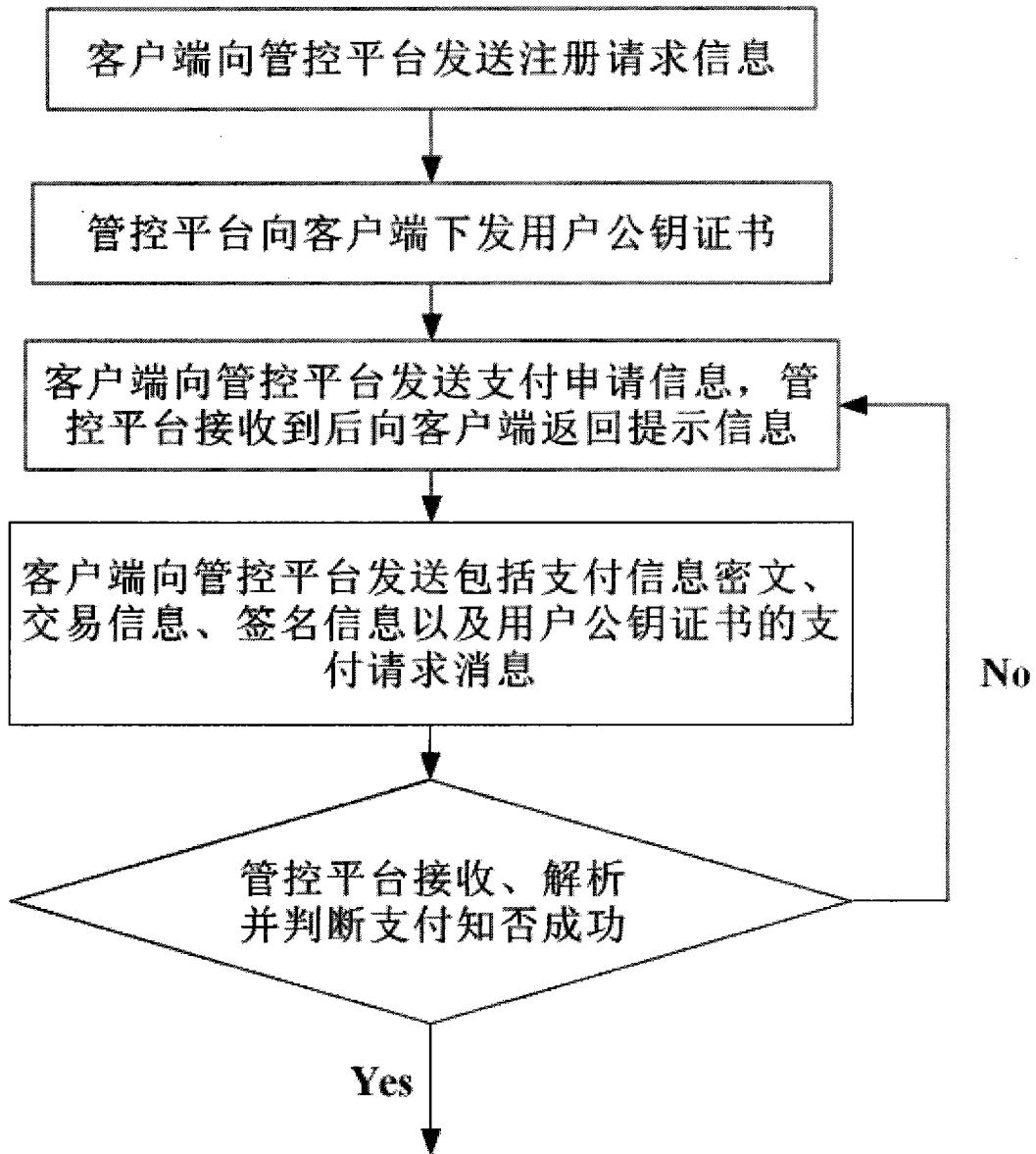


图 1