(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 111639325 B
(45)授权公告日 2023.09.19

(21)申请号 202010469290.X

(22)申请日 2020.05.28

(65)同一申请的已公布的文献号
申请公布号 CN 111639325 A

(43)申请公布日 2020.09.08

(73)专利权人 中国建设银行股份有限公司
地址 100033 北京市西城区金融大街25号

(72)发明人 吴一凡 彭云 杨洋 周军
李承文 黄志敏

(74)专利代理机构 北京品源专利代理有限公司 11332
专利代理师 孟金喆

(51)Int.Cl.
G06F 21/33(2013.01)
G06F 21/60(2013.01)

(56)对比文件
CN 108683700 A,2018.10.19
US 2020119912 A1,2020.04.16
CN 103905376 A,2014.07.02
JP 2013179473 A,2013.09.09
US 2006117181 A1,2006.06.01
US 2011145579 A1,2011.06.16
US 2013117824 A1,2013.05.09
US 2016218875 A1,2016.07.28
US 6871276 B1,2005.03.22

审查员 甄红欣

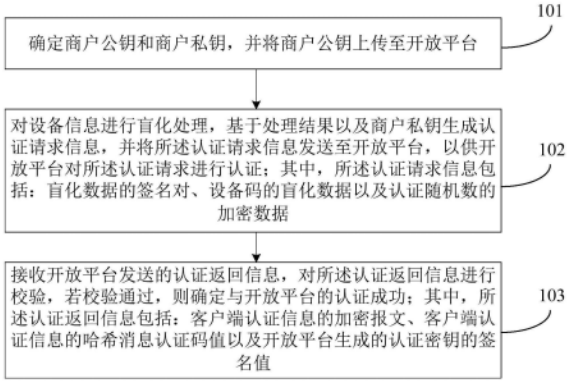
权利要求书4页 说明书16页 附图5页

(54)发明名称

基于开放平台的商户认证方法、装置、设备和存储介质

(57)摘要

本发明实施例公开了一种基于开放平台的商户认证方法、装置、设备和存储介质。该基于开放平台的商户认证方法包括：确定商户公钥和商户私钥，并将商户公钥上传至开放平台；对设备信息进行盲化处理，基于处理结果以及商户私钥生成认证请求信息，并将所述认证请求信息发送至开放平台，以供开放平台对所述认证请求进行认证；接收开放平台发送的认证返回信息，对所述认证返回信息进行校验，若校验通过，则确定与开放平台的认证成功。本发明实施例完成商户的客户端与开放平台的双认证，保证了商户和开放平台的安全性，并且引入盲签名算法，对设备信息盲化处理保障认证过程隐私数据的隐私性。



CN 111639325 B

1.一种基于开放平台的商户认证方法,其特征在于,由商户的客户端执行,包括:

确定商户公钥和商户私钥,并将商户公钥上传至开放平台;

对设备信息进行盲化处理,基于处理结果以及商户私钥生成认证请求信息,并将所述认证请求信息发送至开放平台,以供开放平台对所述认证请求进行认证;其中,所述认证请求信息包括:盲化数据的签名对、设备码的盲化数据以及认证随机数的加密数据;

接收开放平台发送的认证返回信息,对所述认证返回信息进行校验,若校验通过,则确定与开放平台的认证成功;其中,所述认证返回信息包括:客户端认证信息的加密报文、客户端认证信息的哈希消息认证码值以及开放平台生成的认证密钥的签名值;

其中,接收开放平台发送的认证返回信息,对所述认证返回信息进行校验,包括:

使用开放平台公示的平台公钥对所述认证返回信息中的开放平台生成的认证密钥的签名值进行验证有效性;其中,所述签名值是使用平台私钥进行签名确定的;

若验证有效,则对所述认证返回信息中的客户端认证信息的加密报文进行解密,得到解密后的客户端认证信息,其中,所述解密后的客户端认证信息包括开放平台随机数、认证密钥以及有效时间;

根据认证随机数确定解密后的客户端认证信息的哈希消息认证码值,并确定所述解密后的客户端认证信息的哈希消息认证码值与客户端直接接收到的客户端认证信息的哈希消息认证码值的一致性;

根据一致性的确定结果对所述认证返回信息进行校验。

2.根据权利要求1所述的方法,其特征在于,对设备信息进行盲化处理,基于处理结果以及商户私钥生成认证请求信息,并将所述认证请求信息发送至开放平台,包括:

根据设备信息生成设备码;

基于盲化因子对所述设备码进行盲化处理,得到设备码的盲化数据;

使用商户私钥对所述设备码的盲化数据进行签名,得到盲化数据的签名对;其中,所述签名对包括所述盲化数据的签名值和所述盲化因子;

基于开放平台公示的平台公钥对生成的认证随机数进行加密,得到认证随机数的加密数据;

基于所述盲化数据的签名对、设备码的盲化数据以及认证随机数的加密数据,确定认证请求信息,并将所述认证请求信息发送至开放平台。

3.根据权利要求1所述的方法,其特征在于,确定与开放平台的认证成功之后,还包括:

确定解密后的客户端认证信息中的认证通信令牌以及通信令牌的有效时间;

判断通信令牌是否在有效时间内,若是,则确定交易相关信息,并发送所述交易相关信息至开放平台;其中,所述交易相关信息包括交易数据的加密报文、客户端生成的交易随机数、交易数据加密报文的哈希消息认证码值以及通信令牌;

接收开放平台对所述交易相关信息进行处理后返回的交易响应信息,并对所述交易响应信息进行校验,若校验成功,则确定与开放平台的交易完成;其中,所述交易响应信息包括:响应信息的加密报文以及响应信息加密报文的哈希消息认证码值。

4.根据权利要求3所述的方法,其特征在于,确定交易相关信息,并发送所述交易相关信息至开放平台,包括:

对原始交易数据进行加密,得到交易数据的加密报文;其中,加密密钥通过客户端认证

信息进行确定；

根据所述客户端认证信息中的认证随机数确定交易数据加密报文的哈希消息认证码值；

基于所述交易数据的加密报文、交易数据加密报文的哈希消息认证码值、客户端生成的交易随机数以及所述通信令牌，确定交易相关信息，并将所述交易相关信息发送至开放平台。

5.根据权利要求3所述的方法，其特征在于，对所述交易响应信息进行校验，若校验成功，则客户端与开放平台的交易完成，包括：

对接收到的交易响应信息中的所述响应信息的加密报文进行解密，得到解密后的响应信息；

根据所述客户端认证信息中的认证随机数确定接收到的响应信息的加密报文的哈希消息认证码值，并判断所述接收到的响应信息的加密报文的哈希消息认证码值与所述接收到的交易响应信息中的响应信息加密报文的哈希消息认证码值的一致性；

若一致，则校验成功，确定与开放平台的交易完成。

6.一种基于开放平台的商户认证方法，其特征在于，由开放平台执行，包括：

确定平台公钥和平台私钥，并将平台公钥进行公示；

接收客户端发送的认证请求信息，并对所述认证请求信息进行除盲处理，基于处理结果对所述认证请求信息进行校验，并确定校验结果的一致性；其中，所述认证请求信息包括：盲化数据的签名对、设备码的盲化数据以及认证随机数的加密数据；

若一致，则生成认证返回信息，并将所述认证返回信息发送至客户端，用于供商户的客户端进行校验；其中，所述认证返回信息包括：客户端认证信息的加密报文、客户端认证信息的哈希消息认证码值以及开放平台生成的认证密钥的签名值；

其中，生成认证返回信息，并将所述认证返回信息发送至客户端，包括：

基于平台私钥对所述认证随机数的加密数据进行解密，得到解密后的认证随机数；

通过随机数算法生成认证密钥，并使用平台私钥对所述认证密钥进行签名，得到所述认证密钥的签名值；

基于客户端的身份信息、认证随机数、随机生成的通信令牌、盲化数据的签名对中的签名值、认证密钥以及预设通信令牌的有效时间，确定客户端认证信息；

基于平台私钥确定所述认证密钥的签名值，并基于所述认证随机数确定所述客户端认证信息的哈希消息认证码值；

将所述认证随机数作为加密密钥对所述客户端认证信息进行加密，得到客户端认证信息的加密报文；

基于所述客户端认证信息的加密报文、客户端认证信息的哈希消息认证码值以及认证密钥的签名值生成认证返回信息，并将所述认证返回信息发送至客户端。

7.根据权利要求6所述的方法，其特征在于，对所述认证请求信息进行除盲处理，基于处理结果对所述认证请求信息进行校验，并确定校验结果的一致性，包括：

基于所述盲化数据的签名对中的盲化因子对所述设备码的盲化数据进行除盲处理，得到除盲结果，并判断所述除盲结果与盲化数据的签名对中的盲化数据的签名值的一致性；

根据所述一致性判断结果确定校验结果的一致性。

8.根据权利要求6所述的方法，其特征在于，生成认证返回信息，并将所述认证返回信息发送至客户端之后，还包括：

接收客户端发送的交易相关信息，并对所述交易相关信息进行处理；其中，所述交易相关信息包括交易数据的加密报文、客户端生成的交易随机数、交易数据加密报文的哈希消息认证码值以及通信令牌；

根据交易数据处理结果向客户端发送交易响应信息，以供客户端对所述交易响应信息进行校验判断交易是否完成；其中，所述交易响应信息包括：响应信息的加密报文以及响应信息加密报文的哈希消息认证码值。

9.根据权利要求8所述的方法，其特征在于，接收客户端发送的交易相关信息，并对所述交易相关信息进行处理，包括：

接收客户端发送的交易相关信息，并根据所述交易相关信息中的通信令牌判断所述交易随机数是否存在；

若不存在，则将所述交易随机数进行保存，并对交易数据的加密报文进行解密，得到解密后的交易数据；

确定接收到的交易数据的加密报文的哈希消息认证码值，并判断与所述交易相关信息中的交易数据加密报文的哈希消息认证码值的一致性；

若一致，则对所述解密后的交易数据进行处理。

10.根据权利要求8所述的方法，其特征在于，根据交易数据处理结果向客户端发送交易响应信息，包括：

确定对交易数据进行处理后的响应信息；

基于对所述认证随机数的加密数据进行解密后得到的认证随机数和所述认证密钥，对所述响应信息进行加密，得到响应信息的加密报文；

基于所述认证随机数，确定所述响应信息的加密报文的哈希消息认证码值；

基于所述响应信息的加密报文以及响应信息加密报文的哈希消息认证码值确定交易响应信息，并将所述交易响应信息发送至客户端。

11.一种基于开放平台的商户认证装置，其特征在于，由商户的客户端执行，包括：

商户密钥确定模块，用于确定商户公钥和商户私钥，并将商户公钥上传至开放平台；

认证请求信息生成模块，用于对设备信息进行盲化处理，基于处理结果以及商户私钥生成认证请求信息，并将所述认证请求信息发送至开放平台，以供开放平台对所述认证请求进行认证；其中，所述认证请求信息包括：盲化数据的签名对、设备码的盲化数据以及认证随机数的加密数据；

认证返回信息校验模块，用于接收开放平台发送的认证返回信息，对所述认证返回信息进行校验，若校验通过，则确定与开放平台的认证成功；其中，所述认证返回信息包括：客户端认证信息的加密报文、客户端认证信息的哈希消息认证码值以及开放平台生成的认证密钥的签名值；

其中，认证返回信息校验模块，具体用于：

使用开放平台公示的平台公钥对所述认证返回信息中的开放平台生成的认证密钥的签名值进行验证有效性；其中，所述签名值是使用平台私钥进行签名确定的；

若验证有效，则对所述认证返回信息中的客户端认证信息的加密报文进行解密，得到

解密后的客户端认证信息，其中，所述解密后的客户端认证信息包括开放平台随机数、认证密钥以及有效时间；

根据认证随机数确定解密后的客户端认证信息的哈希消息认证码值，并确定所述解密后的客户端认证信息的哈希消息认证码值与客户端直接接收到的客户端认证信息的哈希消息认证码值的一致性；

根据一致性的确定结果对所述认证返回信息进行校验。

12.一种基于开放平台的商户认证装置，其特征在于，由开放平台执行，包括：

平台密钥确定模块，用于确定平台公钥和平台私钥，并将平台公钥进行公示；

认证请求信息校验模块，用于接收客户端发送的认证请求信息，并对所述认证请求信息进行除盲处理，基于处理结果对所述认证请求信息进行校验，并确定校验结果的一致性；其中，所述认证请求信息包括：盲化数据的签名对、设备码的盲化数据以及认证随机数的加密数据；

认证返回信息生成模块，用于若校验结果一致，则生成认证返回信息，并将所述认证返回信息发送至客户端，用于供商户的客户端进行校验；其中，所述认证返回信息包括：客户端认证信息的加密报文、客户端认证信息的哈希消息认证码值以及开放平台生成的认证密钥的签名值；

其中，认证返回信息生成模块，具体用于：

基于平台私钥对所述认证随机数的加密数据进行解密，得到解密后的认证随机数；

通过随机数算法生成认证密钥，并使用平台私钥对所述认证密钥进行签名，得到所述认证密钥的签名值；

基于客户端的身份信息、认证随机数、随机生成的通信令牌、盲化数据的签名对中的签名值、认证密钥以及预设通信令牌的有效时间，确定客户端认证信息；

基于平台私钥确定所述认证密钥的签名值，并基于所述认证随机数确定所述客户端认证信息的哈希消息认证码值；

将所述认证随机数作为加密密钥对所述客户端认证信息进行加密，得到客户端认证信息的加密报文；

基于所述客户端认证信息的加密报文、客户端认证信息的哈希消息认证码值以及认证密钥的签名值生成认证返回信息，并将所述认证返回信息发送至客户端。

13.一种设备，其特征在于，包括：

一个或多个处理器；

存储装置，用于存储一个或多个程序，

当所述一个或多个程序被所述一个或多个处理器执行，使得所述一个或多个处理器实现如权利要求1-5中任一所述的基于开放平台的商户认证方法或如权利要求6-10中任一所述的基于开放平台的商户认证方法。

14.一种计算机可读存储介质，其上存储有计算机程序，其特征在于，该程序被处理器执行时实现如权利要求1-5中任一所述的基于开放平台的商户认证方法或如权利要求6-10中任一所述的基于开放平台的商户认证方法。

基于开放平台的商户认证方法、装置、设备和存储介质

技术领域

[0001] 本发明实施例涉及互联网技术领域，尤其涉及一种基于开放平台的商户认证方法、装置、设备和存储介质。

背景技术

[0002] 开放API是服务型网站常见的一种应用，网站的服务商将自己的网站服务封装成一系列的API(Application Programming Interface，应用编程接口)开放出去，供第三方商户使用，所开放的API被称作OpenAPI，，提供开放API的平台本身就被称为开放平台。

[0003] 第三方商户通过调用OpenAPI实现在开放平台上的业务逻辑时，常用的安全认证机制包括HTTP Basic、Digest Access、App Secret Key+HMAC、JWT(JSON Web Tokens)、OAuth1.0、OAuth2.0等。但是这些安全认证机制需要携带业务的状态信息或者具体业务场景信息进行认证，无法适合平台级的复杂鉴权场景，多为业务型鉴权场景方案。

发明内容

[0004] 本发明实施例提供一种基于开放平台的商户认证方法、装置、设备和存储介质，实现开放平台中无状态无业务的安全认证，以提高基于开放平台的商户认证的效率和安全性。

[0005] 第一方面，本发明实施例提供了一种基于开放平台的商户认证方法，由商户的客户端执行，包括：

[0006] 确定商户公钥和商户私钥，并将商户公钥上传至开放平台；

[0007] 对设备信息进行盲化处理，基于处理结果以及商户私钥生成认证请求信息，并将所述认证请求信息发送至开放平台，以供开放平台对所述认证请求进行认证；其中，所述认证请求信息包括：盲化数据的签名对、设备码的盲化数据以及认证随机数的加密数据；

[0008] 接收开放平台发送的认证返回信息，对所述认证返回信息进行校验，若校验通过，则确定与开放平台的认证成功；其中，所述认证返回信息包括：客户端认证信息的加密报文、客户端认证信息的哈希消息认证码值以及开放平台生成的认证密钥的签名值。

[0009] 第二方面，本发明实施例提供了一种基于开放平台的商户认证方法，由开放平台执行，包括：

[0010] 确定平台公钥和平台私钥，并将平台公钥进行公示；

[0011] 接收客户端发送的认证请求信息，并对所述认证请求信息进行除盲处理，基于处理结果对所述认证请求信息进行校验，并确定校验结果的一致性；其中，所述认证请求信息包括：盲化数据的签名对、设备码的盲化数据以及认证随机数的加密数据；

[0012] 若一致，则生成认证返回信息，并将所述认证返回信息发送至客户端，用于供商户的客户端进行校验；其中，所述认证返回信息包括：客户端认证信息的加密报文、客户端认证信息的哈希消息认证码值以及开放平台生成的认证密钥的签名值。

[0013] 第三方面，本发明实施例还提供了一种基于开放平台的商户认证装置，由商户的

客户端执行，包括：

[0014] 商户密钥确定模块，用于确定商户公钥和商户私钥，并将商户公钥上传至开放平台；

[0015] 认证请求信息生成模块，用于对设备信息进行盲化处理，基于处理结果以及商户私钥生成认证请求信息，并将所述认证请求信息发送至开放平台，以供开放平台对所述认证请求进行认证；其中，所述认证请求信息包括：盲化数据的签名对、设备码的盲化数据以及认证随机数的加密数据；

[0016] 认证返回信息校验模块，用于接收开放平台发送的认证返回信息，对所述认证返回信息进行校验，若校验通过，则确定与开放平台的认证成功；其中，所述认证返回信息包括：客户端认证信息的加密报文、客户端认证信息的哈希消息认证码值以及开放平台生成的认证密钥的签名值。

[0017] 第四方面，本发明实施例还提供了一种基于开放平台的商户认证装置，由开放平台执行，包括：

[0018] 平台密钥确定模块，用于确定平台公钥和平台私钥，并将平台公钥进行公示；

[0019] 认证请求信息校验模块，用于接收客户端发送的认证请求信息，并对所述认证请求信息进行除盲处理，基于处理结果对所述认证请求信息进行校验，并确定校验结果的一致性；其中，所述认证请求信息包括：盲化数据的签名对、设备码的盲化数据以及认证随机数的加密数据；

[0020] 认证返回信息生成模块，用于若校验结果一致，则生成认证返回信息，并将所述认证返回信息发送至客户端，用于供商户的客户端进行校验；其中，所述认证返回信息包括：客户端认证信息的加密报文、客户端认证信息的哈希消息认证码值以及开放平台生成的认证密钥的签名值。

[0021] 第五方面，本发明实施例还提供了一种设备，包括：

[0022] 一个或多个处理器；

[0023] 存储装置，用于存储一个或多个程序，

[0024] 当所述一个或多个程序被所述一个或多个处理器执行，使得所述一个或多个处理器实现如本发明任一实施例所述的基于开放平台的商户认证方法。

[0025] 第六方面，本发明实施例还提供了一种计算机可读存储介质，其上存储有计算机程序，该程序被处理器执行时实现如本发明任一实施例所述的基于开放平台的商户认证方法。

[0026] 本发明实施例根据对设备信息以及生成的认证随机数进行处理，确定认证请求信息，并发送至开放平台进行认证；并接收开放平台认证成功后发送的认证返回信息，对认证返回信息进行认证，完成商户的客户端与开放平台的双认证，保证了商户和开放平台的安全性，并且引入盲签名算法，对设备信息盲化处理保障认证过程隐私数据的隐私性。并且对于本发明实施例中的客户端与开放平台之间发送的信息具备无状态无业务性的特点，提高了认证的通用性和安全性。

附图说明

[0027] 图1是本发明实施例一中的基于开放平台的商户认证方法的流程图；

[0028] 图2是本发明实施例二中的基于开放平台的商户认证方法的流程图；

[0029] 图3是本发明实施例三中的基于开放平台的商户认证方法的流程图；

[0030] 图4是本发明实施例四中的基于开放平台的商户认证方法的流程图；

[0031] 图5是本发明实施例五中的基于开放平台的商户认证装置的结构示意图；

[0032] 图6是本发明实施例六中的基于开放平台的商户认证装置的结构示意图；

[0033] 图7是本发明实施例七中的设备的结构示意图。

具体实施方式

[0034] 下面结合附图和实施例对本发明作进一步的详细说明。可以理解的是，此处所描述的具体实施例仅仅用于解释本发明，而非对本发明的限定。另外还需要说明的是，为了便于描述，附图中仅示出了与本发明相关的部分而非全部结构。

[0035] 实施例一

[0036] 图1是本发明实施例一中的基于开放平台的商户认证方法的流程图，本实施例可适用于第三方商户调用开放平台提供的OpenAPI时进行安全认证的情况。该方法可以由基于开放平台的商户认证装置来执行，该装置可以采用软件和/或硬件的方式实现，并可配置在商户的客户端中，例如商户的客户端可以是后台服务器等具有通信和计算能力的设备。如图1所示，该方法具体包括：

[0037] 步骤101、确定商户公钥和商户私钥，并将商户公钥上传至开放平台。

[0038] 客户端发起首次认证请求时，会根据加密算法生成商户公钥和商户私钥。示例性的，客户端使用RSA加密算法，随机生成2个大素数p2、q2，计算n2＝p2q2，其欧拉函数φ(n2)＝(p2-1)(q2-1)，选取整数e2，1≤e2<φ(n2)，使得gcd(φ(n2)，e2)＝1，根据e2d2＝1modφ(n2)，得出d2；即得到商户公钥(e2,n2)，商户私钥(d2,n2)。客户端上传商户公钥至开放平台，并留存商户私钥，以便在于开放平台传输信息时进行加密传输，保证信息传输的安全性。只有在开发平台上传其公钥的商户才能进行调用API，保障了对第三方客户端使用权限的校验。

[0039] 步骤102、对设备信息进行盲化处理，基于处理结果以及商户私钥生成认证请求信息，并将所述认证请求信息发送至开放平台，以供开放平台对所述认证请求进行认证；其中，所述认证请求信息包括：盲化数据的签名对、设备码的盲化数据以及认证随机数的加密数据。

[0040] 其中，盲化处理是指利用盲化因子对数据进行加密的处理，其利用随机数生成盲化因子，使用盲化因子将信息进行盲化。使用盲化处理实现对发送信息隐私性的保护。设备信息是指客户端所使用设备的身份信息，可以根据设备的磁盘ID以及MAC地址(Media Access Control Address，媒体存取控制位址或局域网地址)确定。

[0041] 具体的，商户向开放平台发送认证请求信息，以使得开放平台对提交认证请求的商户信息进行确定和校验，判断该商户是否具备对该开放平台访问的权力，因此认证请求信息中需要商户的设备信息，并且为了保证商户设备信息在数据传输时的隐私性，对商户设备信息进行盲化处理。并且为了保证认证信息的全面性，发送至开放平台的认证请求信息中除了对设备码进行盲化处理得到的相关数据外，还包括客户端生成的认证随机数的加密数据，由于认证随机数是由客户端随机生成的，因此可以提高对认证整体过程的安全性

保证。

[0042] 在本实施例中，可选的，对设备信息进行盲化处理，基于处理结果以及商户私钥生成认证请求信息，并将所述认证请求信息发送至开放平台，包括：

[0043] 根据设备信息生成设备码；

[0044] 基于盲化因子对所述设备码进行盲化处理，得到设备码的盲化数据；

[0045] 使用商户私钥对所述设备码的盲化数据进行签名，得到盲化数据的签名对；其中，所述签名对包括所述盲化数据的签名值和所述盲化因子；

[0046] 基于开放平台公示的平台公钥对生成的认证随机数进行加密，得到认证随机数的加密数据；

[0047] 基于所述盲化数据的签名对、设备码的盲化数据以及认证随机数的加密数据，确定认证请求信息，并将所述认证请求信息发送至开放平台。

[0048] 具体的，客户端使用磁盘硬件ID和MAC地址通过Base64编码得到客户端设备唯一ID，记为m＝Base64(磁盘硬件ID+MAC地址)，m即为根据设备信息生成的设备码。Base64是网络上最常见的用于传输8Bit字节码的编码方式之一，Base64是一种基于64个可打印字符来表示二进制数据的方法。

[0049] 客户端使用盲签名算法，生成盲化因子r，基于商户私钥(d2,n2)对客户端设备码m进行盲化处理，m’＝mre(mod n2)，得到设备码的盲化数据m’。再使用商户私钥对盲化数据m’进行签名得到盲签名值s’，即s’＝m’d2(mod n2)，生成盲化数据的签名对(s’,r)。

[0050] 客户端使用UUID算法(Universally Unique Identifier，通用唯一识别码)生成一次性32位认证随机数b，使用开放平台公示的平台公钥(e1,n1)对认证随机数b进行加密得到认证随机数的加密数据c1，即c1＝be1(mod n1)成立。

[0051] 客户端根据上述处理确定认证请求信息，将认证请求信息发送至开放平台。认证请求信中包括{s’,r,m’,c1}。

[0052] 步骤103、接收开放平台发送的认证返回信息，对所述认证返回信息进行校验，若校验通过，则确定与开放平台的认证成功；其中，所述认证返回信息包括：客户端认证信息的加密报文、客户端认证信息的哈希消息认证码值以及开放平台生成的认证密钥的签名值。

[0053] 开放平台接收到客户端发送的认证请求信息后，对认证请求信息进行处理后发送认证返回信息给客户端，该认证返回信息反映了开放平台对客户端此次认证请求的反馈信息。

[0054] 客户端对该反馈信息进行校验，以判断开放平台的认证结果以及对开放平台提供信息的准确性进行校验。开放平台发送的认证返回信息包括客户端认证信息的加密报文E1、客户端认证信息的哈希消息认证码值h1以及开放平台生成的认证密钥的签名值s2，并且对于客户端认证信息D包括开放平台提供给该商户的appid、开放平台生成的开放平台随机数O、盲签名值s’、开放平台生成的认证密钥y以及有效时间t，有效时间表示了该次认证的有效时间。关于开放平台生成认证返回信息的具体过程在实施例三中具体说明，在此不作赘述。

[0055] 在本实施例中，可选的，接收开放平台发送的认证返回信息，对所述认证返回信息进行校验，包括：

[0056] 使用开放平台公示的平台公钥对所述认证返回信息中的开放平台生成的认证密钥的签名值进行验证有效性;其中,所述签名值是使用平台私钥进行签名确定的;

[0057] 若验证有效,则对所述认证返回信息中的客户端认证信息的加密报文进行解密,得到解密后的客户端认证信息,其中,所述解密后的客户端认证信息包括开放平台随机数、认证密钥以及有效时间;

[0058] 根据认证随机数确定解密后的客户端认证信息的哈希消息认证码值,并确定所述解密后的客户端认证信息的哈希消息认证码值与客户端直接接收到的客户端认证信息的哈希消息认证码值的一致性;

[0059] 根据一致性的确定结果对所述认证返回信息进行校验。

[0060] 具体的,根据开放平台生成认证返回信息的具体过程对接收到的认证返回信息进行逆处理。示例性的,客户端接收到开放平台发送的认证返回信息后,使用平台公钥对接收到的s2进行验证有效性,若有效,则对客户端认证信息的加密报文E1进行Base64解码,解码后,使用AES-128-CBC作为解密算法,截取认证随机数b的16进制编码中的前16位作为加密向量,使用认证随机数b作为解密密钥,得到客户端认证信息D中的开放平台提供给该商户的APPID、开放平台生成的开放平台随机数O、盲签名值s'、开放平台生成的认证密钥y以及有效时间t。即使用D<-UnBase64(AES_Decrypt(E1,b,substract(b,0,15)))。

[0061] 客户端使用签名算法得到上述解密后的客户端认证信息D的哈希消息认证码值h1',并确定该值与接收到的认证返回信息中的客户端认证信息的哈希消息认证码值h1是否一致,若不一致则认证失败返回重新认证。示例性的,客户端使用Hmac-sha256算法得出HMAC(b,D)＝sha256(b⊕opad|sha256(b⊕ipad|D)),其中D＝{商户appid,O,s',y,t},ipad为0x36重复256次,opad为0x5c重复256次,将该次计算的哈希消息认证码HMAC(b,D)即为h1',比对h1与h1'是否一致,如不一致则验签失败要求重新认证;若一致则说明客户端与开放平台的相互认证成功,确定客户端认证信息D中的开放平台随机数O作为此次认证成功的通信令牌,该通信令牌的有效期为t。

[0062] 本发明实施例根据对设备信息以及生成的认证随机数进行处理,确定认证请求信息,并发送至开放平台进行认证;并接收开放平台认证成功后发送的认证返回信息,对认证返回信息进行认证,完成商户的客户端与开放平台的双认证,保证了商户和开放平台的安全性,并且引入盲签名算法,对设备信息盲化处理保障认证过程隐私数据的隐私性。并且对于本发明实施例中的客户端与开放平台之间发送的信息具备无状态无业务性的特点,提高了认证的通用性和安全性。

[0063] 实施例二

[0064] 图2是本发明实施例二中的基于开放平台的商户认证方法的流程图,本实施例二在实施例一的基础上进行进一步地优化,对实施例一中步骤103后的步骤进行进一步优化。如图2所示,所述方法包括:

[0065] 步骤201、确定解密后的客户端认证信息中的认证通信令牌以及通信令牌的有效时间。

[0066] 客户端与开放平台认证成功后,确定客户端认证信息D中的开放平台随机数O作为此次认证成功的通信令牌,该通信令牌的有效期为t。由于通信令牌是由开放平台生成的随机数确定的,保证了凭通信令牌进行交易的安全性。

[0067] 步骤202、判断通信令牌是否在有效时间内，若是，则确定交易相关信息，并发送所述交易相关信息至开放平台；其中，所述交易相关信息包括交易数据的加密报文、客户端生成的交易随机数、交易数据加密报文的哈希消息认证码值以及通信令牌。

[0068] 由于通信令牌的有效期为t，则该通信令牌的失效时间为Tr＝Ts+t，Ts为认证成功时的当前系统时间。判断交易时的系统时间Tc是否大于Tr，若是，则说明认证失效需要请求重新认证；若小于等于，则该通信令牌有效后续交易无需再次请求认证。

[0069] 客户端将需要进行交易的报文发送至开放平台，并且为了保证报文发送的安全性，发送的交易相关信息中包括交易数据的加密报文、客户端生成的交易随机数、交易数据加密报文的哈希消息认证码值以及通信令牌。

[0070] 在本实施例中，可选的，确定交易相关信息，并发送所述交易相关信息至开放平台，包括：

[0071] 对原始交易数据进行加密，得到交易数据的加密报文；其中，加密密钥通过客户端认证信息进行确定；

[0072] 根据所述客户端认证信息中的认证随机数确定交易数据加密报文的哈希消息认证码值；

[0073] 基于所述交易数据的加密报文、交易数据加密报文的哈希消息认证码值、客户端生成的交易随机数以及所述通信令牌，确定交易相关信息，并将所述交易相关信息发送至开放平台。

[0074] 对原始交易数据以二进制形式字节流拼接进行编码，对第i笔交易数据记为ji；使用AES-128-CBC作为加密算法，以ji作为加密内容，截取客户端认证信息中的认证随机数b的16进制编码中的前16位作为加密向量，使用客户端认证信息中的认证密钥y作为加密密钥后得到加密二进制字节流Ui，Ui为交易数据的加密报文，即Ui<-AES_Encrypt(ji,y,substract(b,0,15))。

[0075] 客户端使用Hmac-sha256算法得出HMAC(bi,Ui)＝sha256(b⊕opad|sha256(b⊕ipad|Ui))，ipad为0x36重复256次，opad为0x5c重复256次，将该次计算的哈希消息认证码HMAC(b,Ui)即为hi+1。

[0076] 客户端为每次交易生成一个32位随机数c，作为交易的交易随机数，用于防重放攻击，基于所述交易数据的加密报文Ui、交易数据加密报文的哈希消息认证码值hi+1、客户端生成的交易随机数c以及所述通信令牌0，确定交易相关信息{c,Ui,hi+1,0}，并将所述交易相关信息发送至开放平台。

[0077] 步骤203、接收开放平台对所述交易相关信息进行处理后返回的交易响应信息，并对所述交易响应信息进行校验，若校验成功，则确定与开放平台的交易完成；其中，所述交易响应信息包括：响应信息的加密报文以及响应信息加密报文的哈希消息认证码值。

[0078] 客户端将交易相关信息发送至开放平台后，开放平台对该信息进行处理和校验，并将交易数据发送至后端业务系统，后端业务系统收到交易请求后返回数据，开放平台根据该返回数据生成交易响应信息发送至客户端，客户端通过对交易响应信息的校验，得到交易处理结果，同时进一步的校验也保证了交易的安全性。

[0079] 在本实施例中，可选的，对所述交易响应信息进行校验，若校验成功，则客户端与开放平台的交易完成，包括：

[0080] 对接收到的交易响应信息中的所述响应信息的加密报文进行解密，得到解密后的响应信息；

[0081] 根据所述客户端认证信息中的认证随机数确定接收到的响应信息的加密报文的哈希消息认证码值，并判断所述接收到的响应信息的加密报文的哈希消息认证码值与所述接收到的交易响应信息中的响应信息加密报文的哈希消息认证码值的一致性；

[0082] 若一致，则校验成功，确定与开放平台的交易完成。

[0083] 客户端接收到的交易响应信息包括响应信息的加密报文Si以及响应信息加密报文的哈希消息认证码值hi+2。

[0084] 客户端对接收到响应信息的加密报文Si进行解密，即使用AES-128-CBC作为解密算法，截取b的16进制编码中的前16位作为加密向量，使用y作为解密密钥对加密报文Si进行解密得到ki，即ki<-AES_Decrypt(Si,y,substract(b,0,15)))。

[0085] 客户端对交易数据进行完整性验证，使用Hmac-sha256算法得出HMAC(bi,Base64(Si))＝sha256(b⊕opad|sha256(b⊕ipad|Base64(Si)))，ipad为0x36重复256次，opad为0x5c重复256次，将该次计算的哈希消息认证码HMAC(b,Base64(Si))即为hi+2’，比对接收到的交易响应信息中的hi+2与此次计算得到的hi+2’是否一致，如不一致则返回验签失败，要求重发交易；若一致表明第i笔交易有效，即交易完成。

[0086] 本发明实施例通过对客户端发送的交易数据进行加密，并和开发平台完成交易过程的相互认证。任何一笔交易均为全加密交易，任何一笔交易均使用签名算法或哈希消息验证码进行二次校验，保障了交易的防篡改性以及完整性。

[0087] 实施例三

[0088] 图3是本发明实施例三中的基于开放平台的商户认证方法的流程图，本实施例可适用于第三方商户调用开放平台提供的OpenAPI时进行安全认证的情况。该方法可以由基于开放平台的商户认证装置来执行，该装置可以采用软件和/或硬件的方式实现，并可配置在开放平台中，例如开放平台可以是后台服务器等具有通信和计算能力的设备。如图3所示，该方法具体包括：

[0089] 步骤301、确定平台公钥和平台私钥，并将平台公钥进行公示。

[0090] 开放平台一次性生成其永久密钥，使用RSA算法，随机生成2个大素数p1、q1，计算n1＝p1q1，其欧拉函数φ(n1)＝(p1-1)(q1-1)，选取整数e1，1≤e1<φ(n1)，使得gcd(φ(n1),e1)＝1，根据e1d1＝1modφ(n1)，得出d1；即得到平台公钥(e1,n1)，平台私钥(d1,n1)。开放平台在平台公示其平台公钥(e1,n1)，留存平台私钥(d1,n1)。

[0091] 步骤302、接收客户端发送的认证请求信息，并对所述认证请求信息进行除盲处理，基于处理结果对所述认证请求信息进行校验，并确定校验结果的一致性；其中，所述认证请求信息包括：盲化数据的签名对、设备码的盲化数据以及认证随机数的加密数据。

[0092] 开发平台接收到客户端发送的认证请求信息后，对认证请求信息进行除盲处理，基于对除盲处理后的设备码的判断以及对认证随机数的认证，得到校验结果。设备码的校验可以保障开放平台对具体发送交易的异常机器进行快速隔离；而引入盲签名算法，对设备码盲化，去盲保障认证过程隐私数据的隐私性，条件匿名性。

[0093] 在本实施例中，可选的，对所述认证请求信息进行除盲处理，基于处理结果对所述认证请求信息进行校验，并确定校验结果的一致性，包括：

[0094] 基于所述盲化数据的签名对中的盲化因子对所述设备码的盲化数据进行除盲处理，得到除盲结果，并判断所述除盲结果与盲化数据的签名对中的盲化数据的签名值的一致性；

[0095] 根据所述一致性判断结果确定校验结果的一致性。

[0096] 开放平台接收到认证请求信息{s'，r，m'，c1}后，对设备码的盲化数据m'进行除盲处理，即s"＝(m')r-1(mod n1)，比对认证请求信息中的s'与除盲处理后的s"的一致性，如果不一致则认证无效，则明文返回认证失败；若一致则开放平台使用平台私钥(d1，n1)对c1进行解密得到认证随机数b，即b＝c1d1(mod n1)；如果解密失败，则明文返回认证失败，解密成功后即为商户认证成功。

[0097] 步骤303、若一致，则生成认证返回信息，并将所述认证返回信息发送至客户端，用于供商户的客户端进行校验；其中，所述认证返回信息包括：客户端认证信息的加密报文、客户端认证信息的哈希消息认证码值以及开放平台生成的认证密钥的签名值。

[0098] 对认证请求信息校验成功后，开放平台需要生成认证返回信息，该认证返回信息需要对客户端提交的认证信息进行反馈，以便客户端进行二次校验，提高认证的安全性。并且认证返回信息中包括了开放平台生成的认证密钥。开放平台将认证返回信息发送至客户端，以便客户端进行二次校验。

[0099] 在本实施例中，可选的，生成认证返回信息，并将所述认证返回信息发送至客户端，包括：

[0100] 基于平台私钥对所述认证随机数的加密数据进行解密，得到解密后的认证随机数；

[0101] 通过随机数算法生成认证密钥，并使用平台私钥对所述认证密钥进行签名，得到所述认证密钥的签名值；

[0102] 基于客户端的身份信息、认证随机数、随机生成的通信令牌、盲化数据的签名对中的签名值、认证密钥以及预设通信令牌的有效时间，确定客户端认证信息；

[0103] 基于平台私钥确定所述认证密钥的签名值，并基于所述认证随机数确定所述客户端认证信息的哈希消息认证码值；

[0104] 将所述认证随机数作为加密密钥对所述客户端认证信息进行加密，得到客户端认证信息的加密报文；

[0105] 基于所述客户端认证信息的加密报文、客户端认证信息的哈希消息认证码值以及认证密钥的签名值生成认证返回信息，并将所述认证返回信息发送至客户端。

[0106] 解密成功后即为商户认证成功，基于平台私钥对所述认证随机数的加密数据进行解密，得到解密后的认证随机数b，并且开放平台生成32位随机数标记为0作为开放平台随机数，使用随机数算法生成32位认证密钥y，失效期t默认为12小时，内存暂存D＝{商户appid，0，s'，y，t}，可选的，为了标识不同来源的appid可以用Di进行表示，i表示不同的appid，当达到失效期t后，该条数据自动从内存清除。

[0107] 开放平台使用平台私钥(d1，n1)对认证密钥y进行签名得到签名值s2，示例性的，使用消息摘要算法得到y的消息摘要h(y)，得出s2＝(h(y))d1mod n1。

[0108] 计算D的哈希消息认证码值，使用Hmac-sha256算法得出HMAC(b，D)＝sha256(b⊕opad|sha256(b⊕ipad|D))，其中D＝{商户appid，0，s'，y，t}，ipad为0x36重复256次，opad

为0x5c重复256次，将该次计算的哈希消息认证码HMAC(b,D1)即为h1。

[0109] 为了进一步保证加密效果，使用AES-128-CBC作为加密算法，以D作为加密内容，截取认证随机数b的16进制编码中的前16位作为加密向量，使用b作为加密密钥后使用Base64进行编码得到加密报文E1，即E1<-Base64(AES_Encrypt(D1,b,substract(b,0,15)))。

[0110] 认证成功后开放平台将根据上述方法确定的认证返回信息发送至客户端，认证返回信息包含{E1,h1,s2}。

[0111] 本发明实施例根据对客户端发送的认证请求信息进行除盲处理，从而实现对客户端发送的认证请求进行校验，并根据校验结果生成认证返回信息，以便客户端根据开放平台发送的认证返回信息进行校验，判断开放平台对客户端认证结果判断的正确性，完成商户的客户端与开放平台的双认证，保证了商户和开放平台的安全性。

[0112] 实施例四

[0113] 图4是本发明实施例四中的基于开放平台的商户认证方法的流程图，本实施例四在实施例三的基础上进行进一步地优化，对实施例三中步骤303后的步骤进行进一步优化。如图4所示，所述方法包括：

[0114] 步骤401、接收客户端发送的交易相关信息，并对所述交易相关信息进行处理；其中，所述交易相关信息包括交易数据的加密报文、客户端生成的交易随机数、交易数据加密报文的哈希消息认证码值以及通信令牌。

[0115] 客户端与开放平台认证成功后，开放平台可以对客户端发送的交易请求进行处理。具体的，开放平台接收客户端发送的交易相关信息，由于为了保证交易数据的隐私性以及保证交易的安全性，交易相关信息进行了一定的加密处理，因此开放平台需要进行一定的逆处理，并判断交易是否成功。

[0116] 在本实施例中，可选的，接收客户端发送的交易相关信息，并对所述交易相关信息进行处理，包括：

[0117] 接收客户端发送的交易相关信息，并根据所述交易相关信息中的通信令牌判断所述交易随机数是否存在；

[0118] 若不存在，则将所述交易随机数进行保存，并对交易数据的加密报文进行解密，得到解密后的交易数据；

[0119] 确定接收到的交易数据的加密报文的哈希消息认证码值，并判断与所述交易相关信息中的交易数据加密报文的哈希消息认证码值的一致性；

[0120] 若一致，则对所述解密后的交易数据进行处理。

[0121] 平台网关收到交易相关信息{c,Ui,hi+1,0}的二进制字节流后，根据0标识交易来源，查询内存中是否存在c，如果存在，则返回重放交易报文，禁止重复请求，否则在内存中添加c，使用随机数机制，重复的随机数交易不可二次发送，即防重放机制，保障了交易的防重放性。

[0122] 判断c不存在后平台网关对接收到的Ui进行解密，即使用AES-128-CBC作为解密算法，截取认证随机数b的16进制编码中的前16位作为加密向量，使用认证密钥y作为解密密钥解密交易数据的加密报文Ui得到交易数据ji，即ji<-AES_Decrypt(Ui,y,substract(b,0,15)))。

[0123] 对于校验过程中的认证密钥y由服务端生成，验签密钥b由客户端生成，两端共同

管理密钥,使得攻击者难以在中间截获任意一方密钥进行非法操作,提高安全性。

[0124] 平台网关使用Hmac-sha256算法得出HMAC(b,Ui)＝sha256(b⊕opad|sha256(b⊕ipad|Ui)),ipad为0x36重复256次,opad为0x5c重复256次,将该次计算的哈希消息认证码HMAC(b,U1)即为hi+1',比对接收到的交易相关信息中的hi+1与hi+1'一致性,如不一致则返回验签失败,要求重发交易;若hi+1与hi+1'一致,则将ji以报文的形式转发至后端业务系统。

[0125] 步骤402、根据交易数据处理结果向客户端发送交易响应信息,以供客户端对所述交易响应信息进行校验判断交易是否完成;其中,所述交易响应信息包括:响应信息的加密报文以及响应信息加密报文的哈希消息认证码值。

[0126] 平台网关对交易相关信息中的信息进行校验后,确定交易数据的安全性和准确性,继而对交易数据进行处理,并将处理结果发送至客户端,同时为了保证处理结果发送的安全性,需要对响应信息进行加密处理,并将加密处理后的响应信息发送至客户端,以便客户端对其进行二次校验,保证此次交易完成的安全性。

[0127] 在本实施例中,可选的,根据交易数据处理结果向客户端发送交易响应信息,包括:

[0128] 确定对交易数据进行处理后的响应信息;

[0129] 基于对所述认证随机数的加密数据进行解密后得到的认证随机数和所述认证密钥,对所述响应信息进行加密,得到响应信息的加密报文;

[0130] 基于所述认证随机数,确定所述响应信息的加密报文的哈希消息认证码值;

[0131] 基于所述响应信息的加密报文以及响应信息加密报文的哈希消息认证码值确定交易响应信息,并将所述交易响应信息发送至客户端。

[0132] 开放平台将交易数据发送至后端业务系统进行处理,后端业务系统收到请求返回响应ki,则ki为此次交易的响应信息。

[0133] 平台网关以二进制形式字节流拼接进行编码,使用AES-128-CBC作为加密算法,以ki作为加密内容,截取认证随机数b的16进制编码中的前16位作为加密向量,使用认证密钥y作为加密密钥后得到加密二进制字节流Si,Si为响应信息的加密报文,即Si<-AES_Encrypt(ki,y,substract(b,0,15)))。接着平台网关使用Hmac-sha256算法得出HMAC(bi,Base64(Si))＝sha256(b⊕opad|sha256(b⊕ipad|Base64(Si))),ipad为0x36重复256次,opad为0x5c重复256次,将该次计算的哈希消息认证码HMAC(b,Base64(Si))即为hi+2,hi+2为响应信息加密报文的哈希消息认证码值。

[0134] 基于上述加密处理,开放平台将对第i笔交易数据进行响应的信息发送至客户端,其中,交易响应信息为{Si,hi+2}。

[0135] 本发明实施例提供了第三方商户可自行实现算法或通过SDK的形式,实现对其身份的安全验证以及报文的加密解密机制,进而保证用户身份验证、防重放攻击、防报文篡改以及防劫持特性。

[0136] 本发明实施例通过对客户端发送的交易相关信息进行校验,根据校验结果对交易相关信息进行处理,保证了交易的安全性;并且交易处理后,对响应信息也进行加密处理发送至客户端,以便客户端进行二次校验,完成客户端和开发平台完成交易过程的相互认证。在交易过程中任何一笔交易均为全加密交易,均使用签名算法或哈希消息验证码进行二次

校验，保障了交易的防篡改性以及完整性。

[0137] 实施例五

[0138] 图5是本发明实施例五中的基于开放平台的商户认证装置的结构示意图，本实施例可适用于第三方商户调用开放平台提供的OpenAPI时进行安全认证的情况，由商户的客户端执行。如图5所示，该装置包括：

[0139] 商户密钥确定模块510，用于确定商户公钥和商户私钥，并将商户公钥上传至开放平台；

[0140] 认证请求信息生成模块520，用于对设备信息进行盲化处理，基于处理结果以及商户私钥生成认证请求信息，并将所述认证请求信息发送至开放平台，以供开放平台对所述认证请求进行认证；其中，所述认证请求信息包括：盲化数据的签名对、设备码的盲化数据以及认证随机数的加密数据；

[0141] 认证返回信息校验模块530，用于接收开放平台发送的认证返回信息，对所述认证返回信息进行校验，若校验通过，则确定与开放平台的认证成功；其中，所述认证返回信息包括：客户端认证信息的加密报文、客户端认证信息的哈希消息认证码值以及开放平台生成的认证密钥的签名值。

[0142] 本发明实施例根据对设备信息以及生成的认证随机数进行处理，确定认证请求信息，并发送至开放平台进行认证；并接收开放平台认证成功后发送的认证返回信息，对认证返回信息进行认证，完成商户的客户端与开放平台的双认证，保证了商户和开放平台的安全性，并且引入盲签名算法，对设备信息盲化处理保障认证过程隐私数据的隐私性。并且对于本发明实施例中的客户端与开放平台之间发送的信息具备无状态无业务性的特点，提高了认证的通用性和安全性。

[0143] 可选的，认证请求信息生成模块，具体用于：

[0144] 根据设备信息生成设备码；

[0145] 基于盲化因子对所述设备码进行盲化处理，得到设备码的盲化数据；

[0146] 使用商户私钥对所述设备码的盲化数据进行签名，得到盲化数据的签名对；其中，所述签名对包括所述盲化数据的签名值和所述盲化因子；

[0147] 基于开放平台公示的平台公钥对生成的认证随机数进行加密，得到认证随机数的加密数据；

[0148] 基于所述盲化数据的签名对、设备码的盲化数据以及认证随机数的加密数据，确定认证请求信息，并将所述认证请求信息发送至开放平台。

[0149] 可选的，认证返回信息校验模块，具体用于：

[0150] 使用开放平台公示的平台公钥对所述认证返回信息中的开放平台生成的认证密钥的签名值进行验证有效性；其中，所述签名值是使用平台私钥进行签名确定的；

[0151] 若验证有效，则对所述认证返回信息中的客户端认证信息的加密报文进行解密，得到解密后的客户端认证信息，其中，所述解密后的客户端认证信息包括开放平台随机数、认证密钥以及有效时间；

[0152] 根据认证随机数确定解密后的客户端认证信息的哈希消息认证码值，并确定所述解密后的客户端认证信息的哈希消息认证码值与客户端直接接收到的客户端认证信息的哈希消息认证码值的一致性；

[0153] 根据一致性的确定结果对所述认证返回信息进行校验。

[0154] 可选的，所述装置还包括：

[0155] 令牌确定模块，用于确定解密后的客户端认证信息中的认证通信令牌以及通信令牌的有效时间；

[0156] 交易相关信息确定模块，用于判断通信令牌是否在有效时间内，若是，则确定交易相关信息，并发送所述交易相关信息至开放平台；其中，所述交易相关信息包括交易数据的加密报文、客户端生成的交易随机数、交易数据加密报文的哈希消息认证码值以及通信令牌；

[0157] 交易响应信息校验模块，用于接收开放平台对所述交易相关信息进行处理后返回的交易响应信息，并对所述交易响应信息进行校验，若校验成功，则确定与开放平台的交易完成；其中，所述交易响应信息包括：响应信息的加密报文以及响应信息加密报文的哈希消息认证码值。

[0158] 可选的，交易相关信息确定模块，具体用于：

[0159] 对原始交易数据进行加密，得到交易数据的加密报文；其中，加密密钥通过客户端认证信息进行确定；

[0160] 根据所述客户端认证信息中的认证随机数确定交易数据加密报文的哈希消息认证码值；

[0161] 基于所述交易数据的加密报文、交易数据加密报文的哈希消息认证码值、客户端生成的交易随机数以及所述通信令牌，确定交易相关信息，并将所述交易相关信息发送至开放平台。

[0162] 可选的，交易响应信息校验模块，具体用于：

[0163] 对接收到的交易响应信息中的所述响应信息的加密报文进行解密，得到解密后的响应信息；

[0164] 根据所述客户端认证信息中的认证随机数确定接收到的响应信息的加密报文的哈希消息认证码值，并判断所述接收到的响应信息的加密报文的哈希消息认证码值与所述接收到的交易响应信息中的响应信息加密报文的哈希消息认证码值的一致性；

[0165] 若一致，则校验成功，确定与开放平台的交易完成。

[0166] 本发明实施例所提供的基于开放平台的商户认证装置可执行本发明任意实施例所提供的基于开放平台的商户认证方法，具备执行基于开放平台的商户认证方法相应的功能模块和有益效果。

[0167] 实施例六

[0168] 图6是本发明实施例六中的基于开放平台的商户认证装置的结构示意图，本实施例可适用于第三方商户调用开放平台提供的OpenAPI时进行安全认证的情况，由开放平台执行。如图6所示，该装置包括：

[0169] 平台密钥确定模块610，用于确定平台公钥和平台私钥，并将平台公钥进行公示；

[0170] 认证请求信息校验模块620，用于接收客户端发送的认证请求信息，并对所述认证请求信息进行除盲处理，基于处理结果对所述认证请求信息进行校验，并确定校验结果的一致性；其中，所述认证请求信息包括：盲化数据的签名对、设备码的盲化数据以及认证随机数的加密数据；

[0171] 认证返回信息生成模块630，用于若校验结果一致，则生成认证返回信息，并将所述认证返回信息发送至客户端，用于供商户的客户端进行校验；其中，所述认证返回信息包括：客户端认证信息的加密报文、客户端认证信息的哈希消息认证码值以及开放平台生成的认证密钥的签名值。

[0172] 本发明实施例根据对客户端发送的认证请求信息进行除盲处理，从而实现对客户端发送的认证请求进行校验，并根据校验结果生成认证返回信息，以便客户端根据开放平台发送的认证返回信息进行校验，判断开放平台对客户端认证结果判断的正确性，完成商户的客户端与开放平台的双认证，保证了商户和开放平台的安全性。

[0173] 可选的，认证请求信息校验模块，具体用于：

[0174] 基于所述盲化数据的签名对中的盲化因子对所述设备码的盲化数据进行除盲处理，得到除盲结果，并判断所述除盲结果与盲化数据的签名对中的盲化数据的签名值的一致性；

[0175] 根据所述一致性判断结果确定校验结果的一致性。

[0176] 可选的，认证返回信息生成模块，具体用于：

[0177] 基于平台私钥对所述认证随机数的加密数据进行解密，得到解密后的认证随机数；

[0178] 通过随机数算法生成认证密钥，并使用平台私钥对所述认证密钥进行签名，得到所述认证密钥的签名值；

[0179] 基于客户端的身份信息、认证随机数、随机生成的通信令牌、盲化数据的签名对中的签名值、认证密钥以及预设通信令牌的有效时间，确定客户端认证信息；

[0180] 基于平台私钥确定所述认证密钥的签名值，并基于所述认证随机数确定所述客户端认证信息的哈希消息认证码值；

[0181] 将所述认证随机数作为加密密钥对所述客户端认证信息进行加密，得到客户端认证信息的加密报文；

[0182] 基于所述客户端认证信息的加密报文、客户端认证信息的哈希消息认证码值以及认证密钥的签名值生成认证返回信息，并将所述认证返回信息发送至客户端。

[0183] 可选的，所述装置还包括：

[0184] 交易相关信息处理模块，用于接收客户端发送的交易相关信息，并对所述交易相关信息进行处理；其中，所述交易相关信息包括交易数据的加密报文、客户端生成的交易随机数、交易数据加密报文的哈希消息认证码值以及通信令牌；

[0185] 交易响应信息发送模块，用于根据交易数据处理结果向客户端发送交易响应信息，以供客户端对所述交易响应信息进行校验判断交易是否完成；其中，所述交易响应信息包括：响应信息的加密报文以及响应信息加密报文的哈希消息认证码值。

[0186] 可选的，交易相关信息处理模块，具体用于：

[0187] 接收客户端发送的交易相关信息，并根据所述交易相关信息中的通信令牌判断所述交易随机数是否存在；

[0188] 若不存在，则将所述交易随机数进行保存，并对交易数据的加密报文进行解密，得到解密后的交易数据；

[0189] 确定接收到的交易数据的加密报文的哈希消息认证码值，并判断与所述交易相关

信息中的交易数据加密报文的哈希消息认证码值的一致性；

[0190] 若一致，则对所述解密后的交易数据进行处理。

[0191] 可选的，交易响应信息发送模块，具体用于：

[0192] 确定对交易数据进行处理后的响应信息；

[0193] 基于对所述认证随机数的加密数据进行解密后得到的认证随机数和所述认证密钥，对所述响应信息进行加密，得到响应信息的加密报文；

[0194] 基于所述认证随机数，确定所述响应信息的加密报文的哈希消息认证码值；

[0195] 基于所述响应信息的加密报文以及响应信息加密报文的哈希消息认证码值确定交易响应信息，并将所述交易响应信息发送至客户端。

[0196] 本发明实施例所提供的基于开放平台的商户认证装置可执行本发明任意实施例所提供的基于开放平台的商户认证方法，具备执行基于开放平台的商户认证方法相应的功能模块和有益效果。

[0197] 实施例七

[0198] 图7是本发明实施例七提供的一种设备的结构示意图。图7示出了适于用来实现本发明实施方式的示例性设备12的框图。图7显示的设备12仅仅是一个示例，不应对本发明实施例的功能和使用范围带来任何限制。

[0199] 如图7所示，设备12以通用计算设备的形式表现。设备12的组件可以包括但不限于：一个或者多个处理器或者处理单元16，系统存储装置28，连接不同系统组件(包括系统存储装置28和处理单元16)的总线18。

[0200] 总线18表示几类总线结构中的一种或多种，包括存储装置总线或者存储装置控制器，外围总线，图形加速端口，处理器或者使用多种总线结构中的任意总线结构的局域总线。举例来说，这些体系结构包括但不限于工业标准体系结构(ISA)总线，微通道体系结构(MAC)总线，增强型ISA总线、视频电子标准协会(VESA)局域总线以及外围组件互连(PCI)总线。

[0201] 设备12典型地包括多种计算机系统可读介质。这些介质可以是任何能够被设备12访问的可用介质，包括易失性和非易失性介质，可移动的和不可移动的介质。

[0202] 系统存储装置28可以包括易失性存储装置形式的计算机系统可读介质，例如随机存取存储装置(RAM)30和/或高速缓存存储装置32。设备12可以进一步包括其它可移动/不可移动的、易失性/非易失性计算机系统存储介质。仅作为举例，存储系统34可以用于读写不可移动的、非易失性磁介质(图7未显示，通常称为“硬盘驱动器”)。尽管图7中未示出，可以提供用于对可移动非易失性磁盘(例如“软盘”)读写的磁盘驱动器，以及对可移动非易失性光盘(例如CD-ROM，DVD-ROM或者其它光介质)读写的光盘驱动器。在这些情况下，每个驱动器可以通过一个或者多个数据介质接口与总线18相连。存储装置28可以包括至少一个程序产品，该程序产品具有一组(例如至少一个)程序模块，这些程序模块被配置以执行本发明各实施例的功能。

[0203] 具有一组(至少一个)程序模块42的程序/实用工具40，可以存储在例如存储装置28中，这样的程序模块42包括但不限于操作系统、一个或者多个应用程序、其它程序模块以及程序数据，这些示例中的每一个或某种组合中可能包括网络环境的实现。程序模块42通常执行本发明所描述的实施例中的功能和/或方法。

[0204] 设备12也可以与一个或多个外部设备14(例如键盘、指向设备、显示器24等)通信，还可与一个或者多个使得用户能与该设备12交互的设备通信，和/或与使得该设备12能与一个或多个其它计算设备进行通信的任何设备(例如网卡，调制解调器等等)通信。这种通信可以通过输入/输出(I/O)接口22进行。并且，设备12还可以通过网络适配器20与一个或者多个网络(例如局域网(LAN)，广域网(WAN)和/或公共网络，例如因特网)通信。如图7所示，网络适配器20通过总线18与设备12的其它模块通信。应当明白，尽管图7中未示出，可以结合设备12使用其它硬件和/或软件模块，包括但不限于：微代码、设备驱动器、冗余处理单元、外部磁盘驱动阵列、RAID系统、磁带驱动器以及数据备份存储系统等。

[0205] 处理单元16通过运行存储在系统存储装置28中的程序，从而执行各种功能应用以及数据处理，例如实现本发明实施例所提供的基于开放平台的商户认证方法，由商户的客户端执行，包括：

[0206] 确定商户公钥和商户私钥，并将商户公钥上传至开放平台；

[0207] 对设备信息进行盲化处理，基于处理结果以及商户私钥生成认证请求信息，并将所述认证请求信息发送至开放平台，以供开放平台对所述认证请求进行认证；其中，所述认证请求信息包括：盲化数据的签名对、设备码的盲化数据以及认证随机数的加密数据；

[0208] 接收开放平台发送的认证返回信息，对所述认证返回信息进行校验，若校验通过，则确定与开放平台的认证成功；其中，所述认证返回信息包括：客户端认证信息的加密报文、客户端认证信息的哈希消息认证码值以及开放平台生成的认证密钥的签名值。或实现本发明实施例所提供的基于开放平台的商户认证方法，由开放平台执行，包括：

[0209] 确定平台公钥和平台私钥，并将平台公钥进行公示；

[0210] 接收客户端发送的认证请求信息，并对所述认证请求信息进行除盲处理，基于处理结果对所述认证请求信息进行校验，并确定校验结果的一致性；其中，所述认证请求信息包括：盲化数据的签名对、设备码的盲化数据以及认证随机数的加密数据；

[0211] 若一致，则生成认证返回信息，并将所述认证返回信息发送至客户端，用于供商户的客户端进行校验；其中，所述认证返回信息包括：客户端认证信息的加密报文、客户端认证信息的哈希消息认证码值以及开放平台生成的认证密钥的签名值。

[0212] 实施例八

[0213] 本发明实施例八还提供了一种计算机可读存储介质，其上存储有计算机程序，该程序被处理器执行时实现如本发明实施例所提供的基于开放平台的商户认证方法，由商户的客户端执行，包括：

[0214] 确定商户公钥和商户私钥，并将商户公钥上传至开放平台；

[0215] 对设备信息进行盲化处理，基于处理结果以及商户私钥生成认证请求信息，并将所述认证请求信息发送至开放平台，以供开放平台对所述认证请求进行认证；其中，所述认证请求信息包括：盲化数据的签名对、设备码的盲化数据以及认证随机数的加密数据；

[0216] 接收开放平台发送的认证返回信息，对所述认证返回信息进行校验，若校验通过，则确定与开放平台的认证成功；其中，所述认证返回信息包括：客户端认证信息的加密报文、客户端认证信息的哈希消息认证码值以及开放平台生成的认证密钥的签名值。或实现本发明实施例所提供的基于开放平台的商户认证方法，由开放平台执行，包括：

[0217] 确定平台公钥和平台私钥，并将平台公钥进行公示；

[0218] 接收客户端发送的认证请求信息，并对所述认证请求信息进行除盲处理，基于处理结果对所述认证请求信息进行校验，并确定校验结果的一致性；其中，所述认证请求信息包括：盲化数据的签名对、设备码的盲化数据以及认证随机数的加密数据；

[0219] 若一致，则生成认证返回信息，并将所述认证返回信息发送至客户端，用于供商户的客户端进行校验；其中，所述认证返回信息包括：客户端认证信息的加密报文、客户端认证信息的哈希消息认证码值以及开放平台生成的认证密钥的签名值。

[0220] 本发明实施例的计算机存储介质，可以采用一个或多个计算机可读的介质的任意组合。计算机可读介质可以是计算机可读信号介质或者计算机可读存储介质。计算机可读存储介质例如可以是——但不限于——电、磁、光、电磁、红外线、或半导体的系统、装置或器件，或者任意以上的组合。计算机可读存储介质的更具体的例子(非穷举的列表)包括：具有一个或多个导线的电连接、便携式计算机磁盘、硬盘、随机存取存储器(RAM)、只读存储器(ROM)、可擦式可编程只读存储器(EPROM或闪存)、光纤、便携式紧凑磁盘只读存储器(CD-ROM)、光存储器件、磁存储器件、或者上述的任意合适的组合。在本文件中，计算机可读存储介质可以是任何包含或存储程序的有形介质，该程序可以被指令执行系统、装置或者器件使用或者与其结合使用。

[0221] 计算机可读的信号介质可以包括在基带中或者作为载波一部分传播的数据信号，其中承载了计算机可读的程序代码。这种传播的数据信号可以采用多种形式，包括但不限于电磁信号、光信号或上述的任意合适的组合。计算机可读的信号介质还可以是计算机可读存储介质以外的任何计算机可读介质，该计算机可读介质可以发送、传播或者传输用于由指令执行系统、装置或者器件使用或者与其结合使用的程序。

[0222] 计算机可读介质上包含的程序代码可以用任何适当的介质传输，包括——但不限于无线、电线、光缆、RF等等，或者上述的任意合适的组合。

[0223] 可以以一种或多种程序设计语言或其组合来编写用于执行本发明操作的计算机程序代码，所述程序设计语言包括面向对象的程序设计语言—诸如Java、Smalltalk、C++，还包括常规的过程式程序设计语言—诸如”C”语言或类似的程序设计语言。程序代码可以完全地在用户计算机上执行、部分地在用户计算机上执行、作为一个独立的软件包执行、部分在用户计算机上部分在远程计算机上执行、或者完全在远程计算机或服务器上执行。在涉及远程计算机的情形中，远程计算机可以通过任意种类的网络——包括局域网(LAN)或广域网(WAN)—连接到用户计算机，或者，可以连接到外部计算机(例如利用因特网服务提供商来通过因特网连接)。

[0224] 注意，上述仅为本发明的较佳实施例及所运用技术原理。本领域技术人员会理解，本发明不限于这里所述的特定实施例，对本领域技术人员来说能够进行各种明显的变化、重新调整和替代而不会脱离本发明的保护范围。因此，虽然通过以上实施例对本发明进行了较为详细的说明，但是本发明不仅仅限于以上实施例，在不脱离本发明构思的情况下，还可以包括更多其他等效实施例，而本发明的范围由所附的权利要求范围决定。

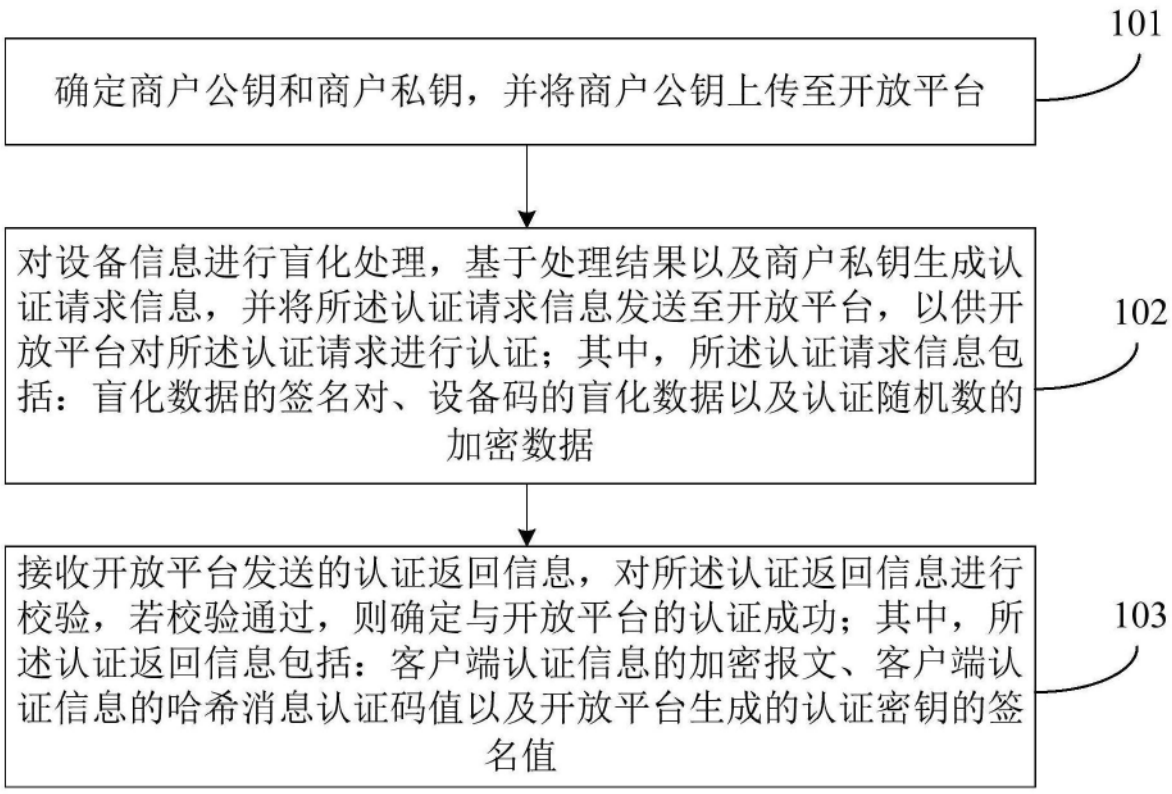

101
确定商户公钥和商户私钥，并将商户公钥上传至开放平台
对设备信息进行盲化处理，基于处理结果以及商户私钥生成认证请求信息，并将所述认证请求信息发送至开放平台，以供开放平台对所述认证请求进行认证；其中，所述认证请求信息包括：盲化数据的签名对、设备码的盲化数据以及认证随机数的加密数据
102
接收开放平台发送的认证返回信息，对所述认证返回信息进行校验，若校验通过，则确定与开放平台的认证成功；其中，所述认证返回信息包括：客户端认证信息的加密报文、客户端认证信息的哈希消息认证码值以及开放平台生成的认证密钥的签名值
103

图1

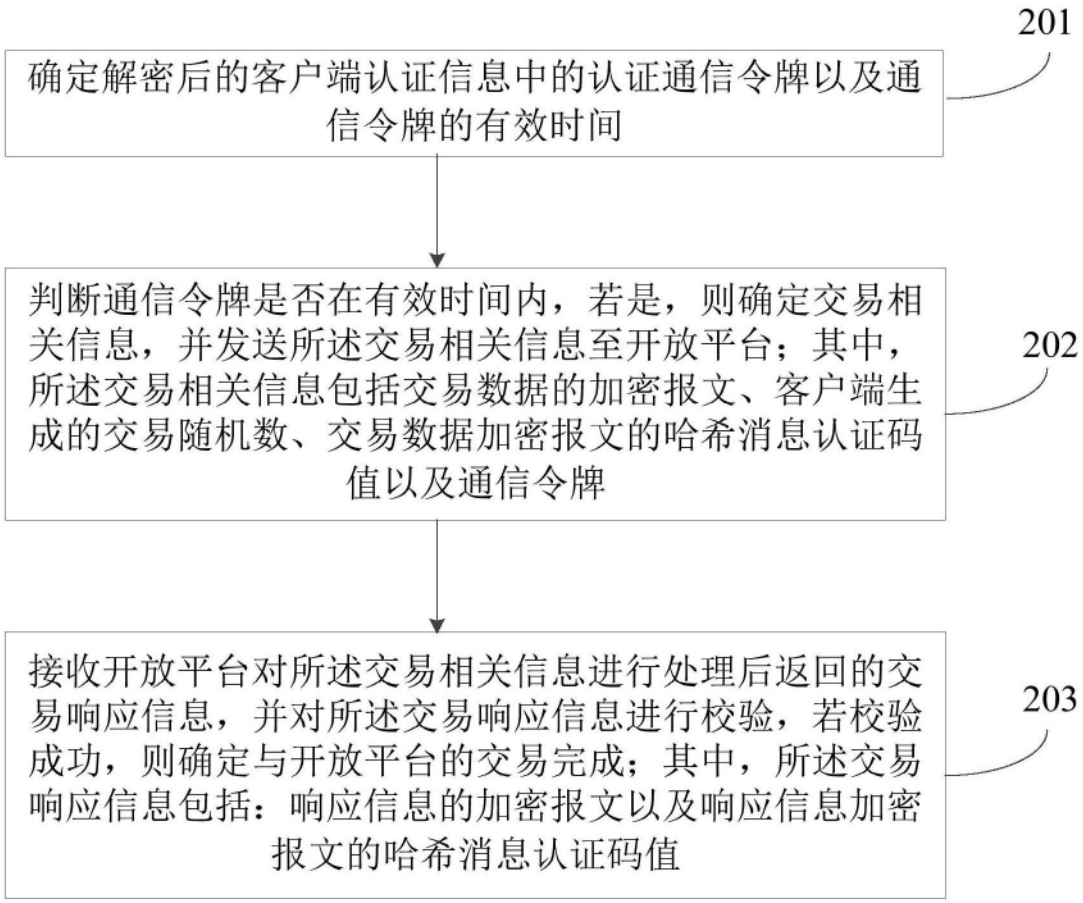

201
确定解密后的客户端认证信息中的认证通信令牌以及通信令牌的有效时间
202
判断通信令牌是否在有效时间内，若是，则确定交易相关信息，并发送所述交易相关信息至开放平台；其中，所述交易相关信息包括交易数据的加密报文、客户端生成的交易随机数、交易数据加密报文的哈希消息认证码值以及通信令牌
203
接收开放平台对所述交易相关信息进行处理后返回的交易响应信息，并对所述交易响应信息进行校验，若校验成功，则确定与开放平台的交易完成；其中，所述交易响应信息包括：响应信息的加密报文以及响应信息加密报文的哈希消息认证码值

图2

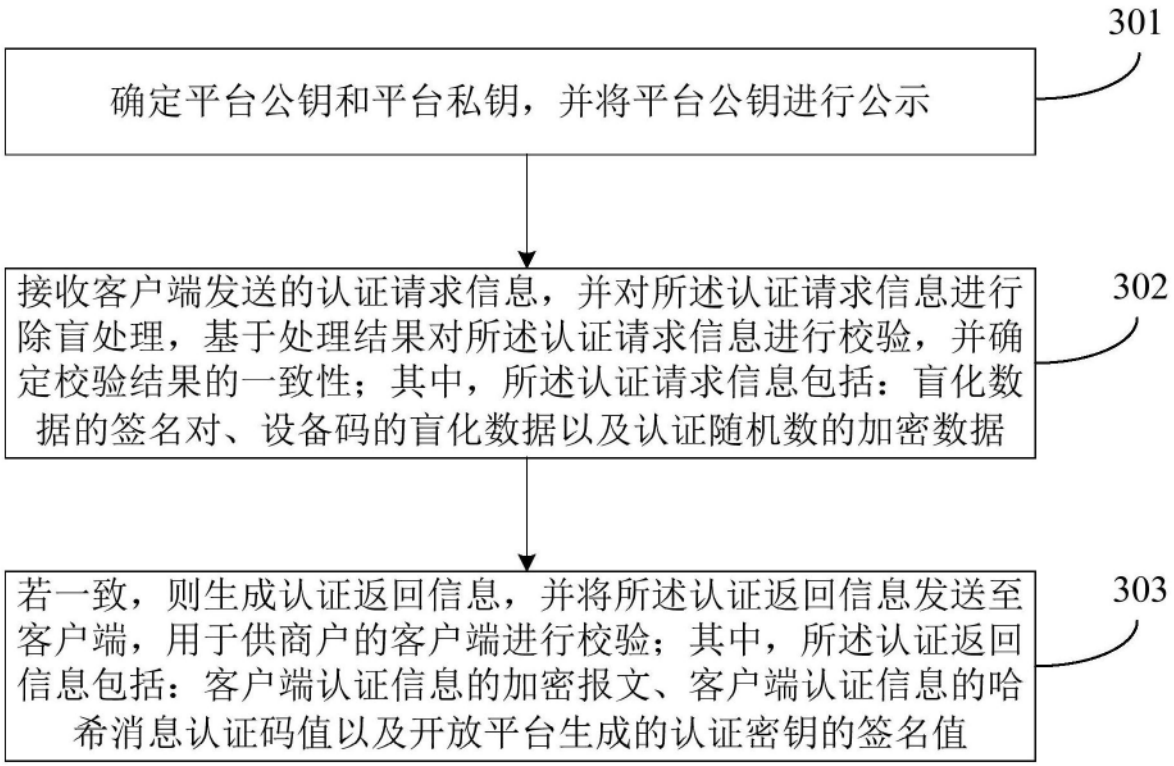

301
确定平台公钥和平台私钥，并将平台公钥进行公示
302
接收客户端发送的认证请求信息，并对所述认证请求信息进行除盲处理，基于处理结果对所述认证请求信息进行校验，并确定校验结果的一致性；其中，所述认证请求信息包括：盲化数据的签名对、设备码的盲化数据以及认证随机数的加密数据
303
若一致，则生成认证返回信息，并将所述认证返回信息发送至客户端，用于供商户的客户端进行校验；其中，所述认证返回信息包括：客户端认证信息的加密报文、客户端认证信息的哈希消息认证码值以及开放平台生成的认证密钥的签名值

图3

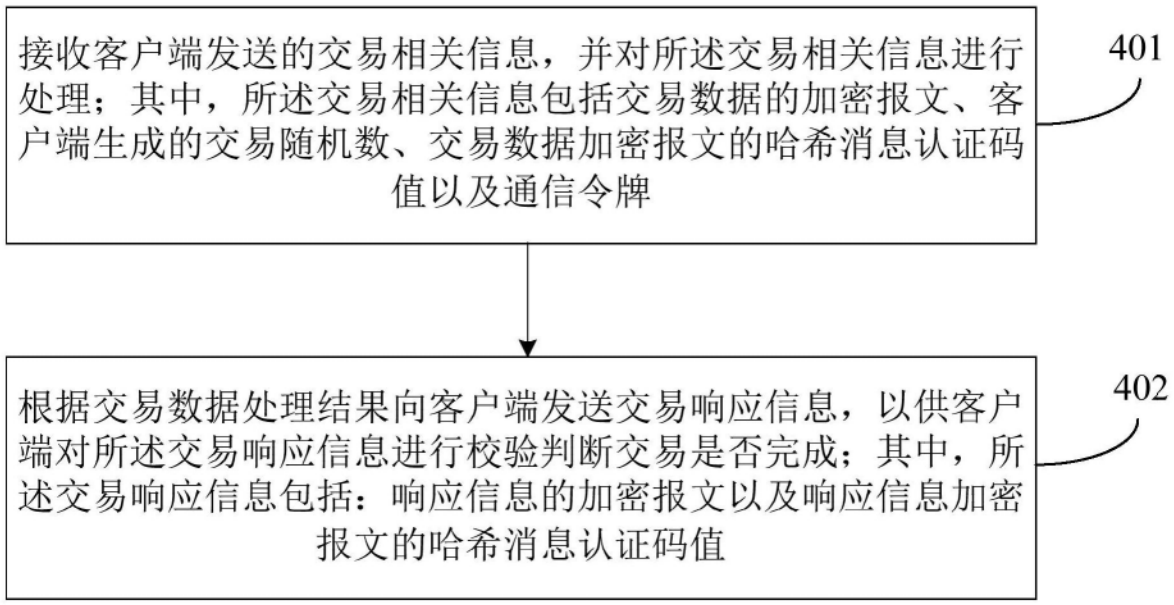

401
接收客户端发送的交易相关信息，并对所述交易相关信息进行处理；其中，所述交易相关信息包括交易数据的加密报文、客户端生成的交易随机数、交易数据加密报文的哈希消息认证码值以及通信令牌
402
根据交易数据处理结果向客户端发送交易响应信息，以供客户端对所述交易响应信息进行校验判断交易是否完成；其中，所述交易响应信息包括：响应信息的加密报文以及响应信息加密报文的哈希消息认证码值

图4


商户密钥确定模块
510
认证请求信息生成模块
520
认证返回信息校验模块
530

图5


平台密钥确定模块
610
认证请求信息校验模块
620
认证返回信息生成模块
630

图6

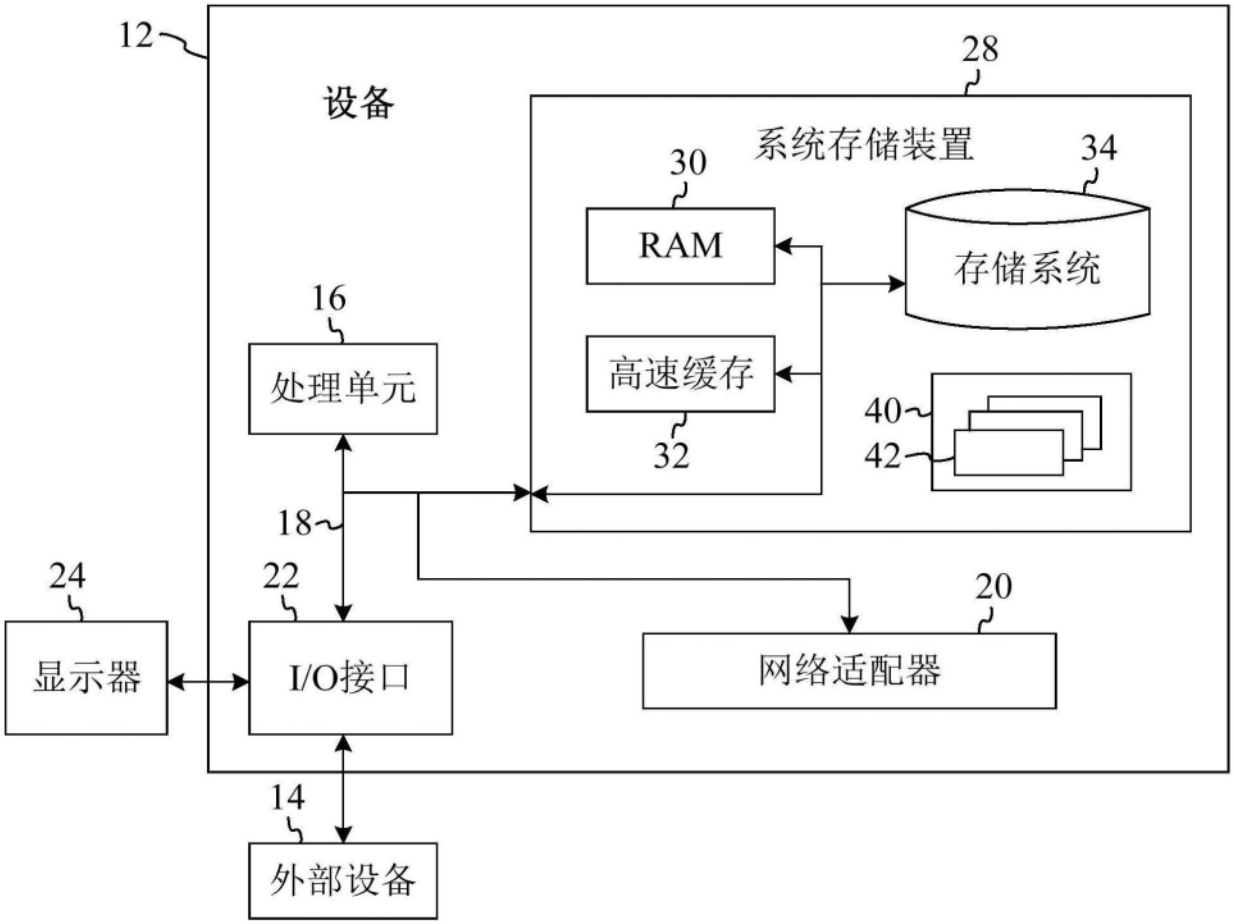

12
设备
28
系统存储装置
30
RAM
34
存储系统
16
处理单元
高速缓存
32
40
42
18
24
22
20
显示器
I/O接口
网络适配器
14
外部设备

图7