(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 111917536 A
(43)申请公布日 2020.11.10

(21)申请号 201910384523.3

(22)申请日 2019.05.09

(71)申请人 北京车和家信息技术有限公司
地址 100102 北京市朝阳区望京街10号院3号楼8层801室

(72)发明人 马东辉 张永新

(74)专利代理机构 北京鼎佳达知识产权代理事务所(普通合伙) 11348
代理人 王伟锋 刘铁生

(51)Int.Cl.
H04L 9/08(2006.01)
H04L 29/06(2006.01)
H04L 9/32(2006.01)

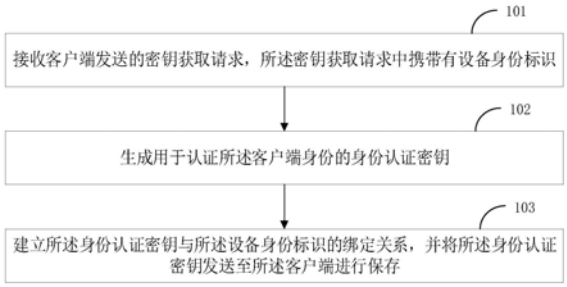
权利要求书4页 说明书19页 附图7页

(54)发明名称

身份认证密钥的生成方法、身份认证的方法、装置及系统

(57)摘要

本公开的实施例公开了一种身份认证密钥的生成方法、身份认证的方法、装置及系统，涉及身份认证技术领域，主要目的在于在不对终端设备内置预设密钥的情况下，提高终端设备身份认的安全性。方法包括：接收客户端发送的密钥获取请求，密钥获取请求中携带有设备身份标识；生成用于认证客户端身份的身份认证密钥；建立身份认证密钥与设备身份标识的绑定关系，并将身份认证密钥发送至客户端进行保存。相对于现有技术，软件厂商无需与终端设备的生产厂商合作，而是当用户在使用软件(客户端)时候，为客户端配属与客户端的设备身份标识绑定的身份认证密钥，可以使服务器通过查询与设备身份标识之间建立的绑定关系的身份认证密钥对客户端进行身份认证。



CN 111917536 A

1.一种身份认证密钥的生成方法,其特征在于,所述方法包括:

接收客户端发送的密钥获取请求,所述密钥获取请求中携带有设备身份标识;

生成用于认证所述客户端身份的身份认证密钥;

建立所述身份认证密钥与所述设备身份标识的绑定关系,并将所述身份认证密钥发送至所述客户端进行保存。

2.根据权利要求1所述的方法,其特征在于,在接收客户端发送的密钥获取请求之前,还包括:

在接收到所述客户端发送的设备身份标识获取请求后,为所述客户端创建设备身份标识;

将所述设备身份标识发送给所述客户端。

3.根据权利要求1所述的方法,其特征在于,当所述密钥获取请求中携带的设备身份标识是使用所述客户端预设的加密密钥加密后的设备身份标识时,在生成用于认证所述客户端身份的身份认证密钥之前,还包括:

使用所述客户端预设的加密密钥所对应的解密密钥对加密后的设备身份标识进行解密;

生成用于认证所述客户端身份的身份认证密钥包括:

若解密成功,则生成所述身份认证密钥。

4.根据权利要求3所述的方法,其特征在于,当所述密钥获取请求中还携带使用所述客户端预设的签名密钥签名后的签名信息时,若解密成功,则在生成所述身份认证密钥之前,所述方法还包括:

使用所述客户端预设的验签密钥对所述签名信息进行验签;

若验签通过,则生成所述身份认证密钥。

5.根据权利要求1所述的方法,其特征在于,建立所述身份认证密钥与所述设备身份标识的绑定关系,包括:

直接建立所述身份认证密钥与所述设备身份标识的绑定关系;

或者,

建立所述身份认证密钥与所述设备身份标识的预绑定关系,并将预绑定的身份认证密钥发送至所述客户端,接收所述客户端发送的密钥验证请求,所述密钥验证请求中携带设备身份标识、利用身份认证密钥加密后的验证信息,查找与所述设备身份标识预绑定关系对应的身份认证密钥,并通过使用查找到的身份认证密钥对所述验证信息进行解密,来对所述客户端进行密钥验证,若密钥验证通过,修改所述身份认证密钥与所述设备身份标识的预绑定关系为绑定关系。

6.根据权利要求1所述的方法,其特征在于,将所述身份认证密钥发送至所述客户端进行保存,具体为:

使用所述客户端中预设的加密密钥对所述身份认证密钥加密后发送至客户端,以便所述客户端利用预设的解密密钥对接收到的身份认证密钥进行解密后,对解密后的身份认证密钥进行保存。

7.一种身份认证密钥的生成方法,其特征在于,所述方法包括:

将密钥获取请求发送给服务器,以便所述服务器生成用于认证客户端身份的身份认证

密钥,并建立所述身份认证密钥与所述密钥获取请求中携带的设备身份标识的绑定关系;

接收并保存所述服务器发送的身份认证密钥。

8.根据权利要求7所述的方法,其特征在于,在将密钥获取请求发送给服务器之前,还包括:

将设备身份标识获取请求发送给服务器,以便所述服务器创建设备身份标识;

接收所述服务器发送的设备身份标识。

9.根据权利要求7所述的方法,其特征在于,将密钥获取请求发送给服务器,以便所述服务器生成用于认证客户端身份的身份认证密钥,包括:

使用客户端预设的加密密钥加密所述设备身份标识;

将携带加密后的设备身份标识的密钥获取请求发送给服务器,以便服务器使用所述客户端预设的加密密钥所对应的解密密钥对加密后的设备身份标识进行解密,若解密成功,生成所述身份认证密钥。

10.根据权利要求9所述的方法,其特征在于,若解密成功,生成所述身份认证密钥之前,还包括:

使用所述客户端预设的签名密钥签名生成签名信息;

将携带签名信息的密钥获取请求发送给服务器,以便服务器使用所述客户端预设的验签密钥对所述签名信息进行验签,若验签通过,生成所述身份认证密钥。

11.根据权利要求7所述的方法,其特征在于,接收并保存所述服务器发送的身份认证密钥,包括:

接收并直接保存所述服务器发送的身份认证密钥;

或者,

接收所述服务器发送的身份认证密钥后,向服务器发送密钥验证请求,所述密钥验证请求中携带设备身份标识、利用身份认证密钥加密后的验证信息,以使服务器查找与所述设备身份标识具有预绑定关系的身份认证密钥,并通过使用查找到的身份认证密钥对所述验证信息进行解密,来对所述客户端进行密钥验证,若密钥验证通过,修改所述身份认证密钥与所述设备身份标识的预绑定关系为绑定关系;接收所述服务器发送的密钥验证通过信息后,保存所述服务器发送的身份认证密钥。

12.根据权利要求1所述的方法,其特征在于,接收并保存所述服务器发送的身份认证密钥,具体为:

利用预设的解密密钥对接收到的身份认证密钥进行解密后,对解密后的身份认证密钥进行保存。

13.一种身份认证的方法,其特征在于,所述方法包括:

接收客户端发送的经身份认证密钥加密后的客户端身份认证请求和设备身份标识,所述身份认证密钥由权利要求1-6中任一所述的方法生成;

查找所述设备身份标识对应的身份认证密钥;

并通过使用查找到的身份认证密钥对所述加密后的客户端身份认证请求进行解密,来对所述客户端进行身份验证。

14.一种身份认证的方法,其特征在于,所述方法包括:

获取身份认证密钥,所述身份认证密钥由权利要求7-12中任一所述的方法生成;

使用所述身份认证密钥对客户端身份认证请求进行加密；

携带设备身份标识将加密后的客户端身份认证请求发送给服务器，以便所述服务器查找所述设备身份标识对应的身份认证密钥，并通过使用查找到的身份认证密钥对所述加密后的客户端身份认证请求进行解密，来对客户端进行身份验证。

15.一种身份认证密钥的生成装置，其特征在于，所述装置包括：

接收单元，用于接收客户端发送的密钥获取请求，所述密钥获取请求中携带有设备身份标识；

生成单元，用于生成用于认证所述客户端身份的身份认证密钥；

建立单元，用于建立所述身份认证密钥与所述设备身份标识的绑定关系，

发送单元，用于将所述身份认证密钥发送至所述客户端进行保存。

16.一种身份认证密钥的生成装置，其特征在于，所述装置包括：

发送单元，用于将密钥获取请求发送给服务器，以便所述服务器生成用于认证客户端身份的身份认证密钥，并建立所述身份认证密钥与所述密钥获取请求中携带的设备身份标识的绑定关系；

保存单元，用于接收并保存所述服务器发送的身份认证密钥。

17.一种身份认证的装置，其特征在于，所述装置包括：

接收单元，用于接收客户端发送的经身份认证密钥加密后的客户端身份认证请求和设备身份标识，所述身份认证密钥由权利要求1-6中任一所述的方法生成；

查找单元，用于查找所述设备身份标识对应的身份认证密钥；

身份验证单元，用于通过使用查找到的身份认证密钥对所述加密后的客户端身份认证请求进行解密，来对所述客户端进行身份验证。

18.一种身份认证的装置，其特征在于，所述装置包括：

获取单元，用于获取身份认证密钥，所述身份认证密钥由权利要求7-12中任一所述的方法生成；

加密单元，用于使用所述身份认证密钥对客户端身份认证请求进行加密；

发送单元，用于携带设备身份标识将加密后的客户端身份认证请求发送给服务器，以便所述服务器查找所述设备身份标识对应的身份认证密钥，并通过使用查找到的身份认证密钥对所述加密后的客户端身份认证请求进行解密，来对客户端进行身份验证。

19.一种身份认证密钥的生成系统，其特征在于，包括：终端和服务器；

所述服务器包括权利要求15所述的身份认证密钥的生成装置；

所述终端包括权利要求16所述的身份认证密钥的生成装置。

20.一种身份认证的系统，其特征在于，包括：终端和服务器；

所述服务器包括权利要求17所述的身份认证的装置；

所述终端包括权利要求18所述的身份认证的装置。

21.一种车辆，其特征在于，包括上述权利要求16所述的身份认证密钥的生成装置。

22.一种车辆，其特征在于，包括上述权利要求18所述的身份认证的装置。

23.一种身份认证密钥的生成系统，其特征在于，包括：车辆和服务器；

所述服务器包括权利要求15所述的身份认证密钥的生成装置；

所述车辆包括权利要求16所述的身份认证密钥的生成装置。

24.一种身份认证的系统,其特征在于,包括:车辆和服务器;

所述服务器包括权利要求17所述的身份认证密钥的生成装置;

所述车辆包括权利要求18所述的身份认证的装置。

身份认证密钥的生成方法、身份认证的方法、装置及系统

技术领域

[0001] 本公开的实施例涉及身份认证技术领域，特别是涉及一种身份认证密钥的生成方法、身份认证的方法、装置及系统。

背景技术

[0002] 基于互联网的发展，用户通过终端设备(如手机、笔记本电脑、平板电脑、台式机等)在因特网上与外部的设备进行信息交互之前，需要对用户的身份进行认证，认证之后，即可进行诸如网上购物、资产理财等在线交易的操作，使用起来方便快捷。

[0003] 目前的身份认证技术中，普遍采用的方案一种是，用户方保存有私有的账号和密码，用户通过在终端设备的登陆界面中输入账号和密码来向远程服务器进行身份认证。此种方案中，若用户方保存有私有的账号和密码通过木马等非法手段被人窃取，被窃取的账号和密码则可在任意的终端设备进行身份认证，安全性较差。

[0004] 另一种是，软件厂商与终端设备的生产厂商合作，在终端设备中预设软件厂商内置预设的密钥，用来进行身份标识。其中，对于在没有和终端设备的生产厂商合作的情况下，上述的软件厂商预设的密钥则无法内置于终端设备中。

发明内容

[0005] 有鉴于此，本公开的实施例提供一种身份认证密钥的生成方法、身份认证的方法、装置及系统，主要目的在于在不对终端设备内置预设密钥的情况下，提高终端设备身份认证的安全性。

[0006] 为达到上述目的，本公开的实施例主要提供如下技术方案：

[0007] 第一方面，本公开的实施例提供了一身份认证密钥的生成方法，所述方法包括：

[0008] 接收客户端发送的密钥获取请求，所述密钥获取请求中携带有设备身份标识；

[0009] 生成用于认证所述客户端身份的身份认证密钥；

[0010] 建立所述身份认证密钥与所述设备身份标识的绑定关系，并将所述身份认证密钥发送至所述客户端进行保存。

[0011] 在一些实施例中，其中在接收客户端发送的密钥获取请求之前，还包括：

[0012] 在接收到所述客户端发送的设备身份标识获取请求后，为所述客户端创建设备身份标识；

[0013] 将所述设备身份标识发送给所述客户端。

[0014] 在一些实施例中，其中当所述密钥获取请求中携带的设备身份标识是使用所述客户端预设的加密密钥加密后的设备身份标识时，在生成用于认证所述客户端身份的身份认证密钥之前，还包括：

[0015] 使用所述客户端预设的加密密钥所对应的解密密钥对加密后的设备身份标识进行解密；

[0016] 生成用于认证所述客户端身份的身份认证密钥包括：

[0017] 若解密成功，则生成所述身份认证密钥。

[0018] 在一些实施例中，其中当所述密钥获取请求中还携带使用所述客户端预设的签名密钥签名后的签名信息时，若解密成功，则在生成所述身份认证密钥之前，所述方法还包括：

[0019] 使用所述客户端预设的验签密钥对所述签名信息进行验签；

[0020] 若验签通过，则生成所述身份认证密钥。

[0021] 在一些实施例中，其中建立所述身份认证密钥与所述设备身份标识的绑定关系，包括：

[0022] 直接建立所述身份认证密钥与所述设备身份标识的绑定关系；

[0023] 或者，

[0024] 建立所述身份认证密钥与所述设备身份标识的预绑定关系，并将预绑定的身份认证密钥发送至所述客户端，接收所述客户端发送的密钥验证请求，所述密钥验证请求中携带设备身份标识、利用身份认证密钥加密后的验证信息，查找与所述设备身份标识预绑定关系对应的身份认证密钥，并通过使用查找到的身份认证密钥对所述验证信息进行解密，来对所述客户端进行密钥验证，若密钥验证通过，修改所述身份认证密钥与所述设备身份标识的预绑定关系为绑定关系。

[0025] 在一些实施例中，其中将所述身份认证密钥发送至所述客户端进行保存，具体为：

[0026] 使用所述客户端中预设的加密密钥对所述身份认证密钥加密后发送至客户端，以便所述客户端利用预设的解密密钥对接收到的身份认证密钥进行解密后，对解密后的身份认证密钥进行保存。

[0027] 第二方面，本公开的实施例提供了一种身份认证密钥的生成方法，所述方法包括：

[0028] 将密钥获取请求发送给服务器，以便所述服务器生成用于认证客户端身份的身份认证密钥，并建立所述身份认证密钥与所述密钥获取请求中携带的设备身份标识的绑定关系；

[0029] 接收并保存所述服务器发送的身份认证密钥。

[0030] 在一些实施例中，其中在将密钥获取请求发送给服务器之前，还包括：

[0031] 将设备身份标识获取请求发送给服务器，以便所述服务器创建设备身份标识；

[0032] 接收所述服务器发送的设备身份标识。

[0033] 在一些实施例中，其中将密钥获取请求发送给服务器，以便所述服务器生成用于认证客户端身份的身份认证密钥，包括：

[0034] 使用客户端预设的加密密钥加密所述设备身份标识；

[0035] 将携带加密后的设备身份标识的密钥获取请求发送给服务器，以便服务器使用所述客户端预设的加密密钥所对应的解密密钥对加密后的设备身份标识进行解密，若解密成功，生成所述身份认证密钥。

[0036] 在一些实施例中，其中若解密成功，生成所述身份认证密钥之前，还包括：

[0037] 使用所述客户端预设的签名密钥签名生成签名信息；

[0038] 将携带签名信息的密钥获取请求发送给服务器，以便服务器使用所述客户端预设的验签密钥对所述签名信息进行验签，若验签通过，生成所述身份认证密钥。

[0039] 在一些实施例中，其中接收并保存所述服务器发送的身份认证密钥，包括：

[0040] 接收并直接保存所述服务器发送的身份认证密钥；

[0041] 或者，

[0042] 接收所述服务器发送的身份认证密钥后，向服务器发送密钥验证请求，所述密钥验证请求中携带设备身份标识、利用身份认证密钥加密后的验证信息，以使服务器查找与所述设备身份标识具有预绑定关系的身份认证密钥，并通过使用查找到的身份认证密钥对所述验证信息进行解密，来对所述客户端进行密钥验证，若密钥验证通过，修改所述身份认证密钥与所述设备身份标识的预绑定关系为绑定关系；接收所述服务器发送的密钥验证通过信息后，保存所述服务器发送的身份认证密钥

[0043] 在一些实施例中，其中接收并保存所述服务器发送的身份认证密钥，具体为：

[0044] 利用预设的解密密钥对接收到的身份认证密钥进行解密后，对解密后的身份认证密钥进行保存。

[0045] 第三方面，本公开的实施例提供了一种身份认证的方法，所述方法包括：

[0046] 接收客户端发送的经身份认证密钥加密后的客户端身份认证请求和设备身份标识，所述身份认证密钥由第一方面所述的方法生成；

[0047] 查找所述设备身份标识对应的身份认证密钥；

[0048] 并通过使用查找到的身份认证密钥对所述加密后的客户端身份认证请求进行解密，来对所述客户端进行身份验证。

[0049] 第四方面，本公开的实施例提供了一种身份认证的方法，所述方法包括：

[0050] 获取身份认证密钥，所述身份认证密钥由第二方面所述的方法生成；

[0051] 使用所述身份认证密钥对客户端身份认证请求进行加密；

[0052] 携带设备身份标识将加密后的客户端身份认证请求发送给服务器，以便所述服务器查找所述设备身份标识对应的身份认证密钥，并通过使用查找到的身份认证密钥对所述加密后的客户端身份认证请求进行解密，来对客户端进行身份验证。

[0053] 第五方面，本公开的实施例提供了一种身份认证密钥的生成装置，所述装置包括：

[0054] 接收单元，用于接收客户端发送的密钥获取请求，所述密钥获取请求中携带有设备身份标识；

[0055] 生成单元，用于生成用于认证所述客户端身份的身份认证密钥；

[0056] 建立单元，用于建立所述身份认证密钥与所述设备身份标识的绑定关系，

[0057] 发送单元，用于将所述身份认证密钥发送至所述客户端进行保存。

[0058] 在一些实施例中，其中还包括：

[0059] 创建单元，用于在接收客户端发送的密钥获取请求之前，在接收到所述客户端发送的设备身份标识获取请求后，为所述客户端创建设备身份标识；

[0060] 所述发送单元，用于将所述设备身份标识发送给所述客户端。

[0061] 在一些实施例中，其中还包括：

[0062] 解密单元，用于当所述密钥获取请求中携带的设备身份标识是使用所述客户端预设的加密密钥加密后的设备身份标识时，在生成用于认证所述客户端身份的身份认证密钥之前，使用所述客户端预设的加密密钥所对应的解密密钥对加密后的设备身份标识进行解密；

[0063] 生成单元具体用于若解密成功，则生成所述身份认证密钥。

[0064] 在一些实施例中，其中还包括：

[0065] 验签单元，用于当所述密钥获取请求中还携带使用所述客户端预设的签名密钥签名后的签名信息时，若解密成功，则在生成所述身份认证密钥之前，使用所述客户端预设的验签密钥对所述签名信息进行验签；

[0066] 生成单元具体用于若验签通过，则生成所述身份认证密钥。

[0067] 在一些实施例中，其中

[0068] 建立单元具体用于直接建立所述身份认证密钥与所述设备身份标识的绑定关系；

[0069] 或者，

[0070] 建立单元具体用于建立所述身份认证密钥与所述设备身份标识的预绑定关系，并将预绑定的身份认证密钥发送至所述客户端，接收所述客户端发送的密钥验证请求，所述密钥验证请求中携带设备身份标识、利用身份认证密钥加密后的验证信息，查找与所述设备身份标识预绑定关系对应的身份认证密钥，并通过使用查找到的身份认证密钥对所述验证信息进行解密，来对所述客户端进行密钥验证，若密钥验证通过，修改所述身份认证密钥与所述设备身份标识的预绑定关系为绑定关系。

[0071] 在一些实施例中，其中

[0072] 建立单元具体用于使用所述客户端中预设的加密密钥对所述身份认证密钥加密后发送至客户端，以便所述客户端利用预设的解密密钥对接收到的身份认证密钥进行解密后，对解密后的身份认证密钥进行保存。

[0073] 第六方面，本公开的实施例提供了一种身份认证密钥的生成装置，所述装置包括：发送单元，用于将密钥获取请求发送给服务器，以便所述服务器生成用于认证客户端身份的身份认证密钥，并建立所述身份认证密钥与所述密钥获取请求中携带的设备身份标识的绑定关系；

[0074] 保存单元，用于接收并保存所述服务器发送的身份认证密钥。

[0075] 在一些实施例中，其中还包括：

[0076] 发送单元，用于在将密钥获取请求发送给服务器之前，将设备身份标识获取请求发送给服务器，以便所述服务器创建设备身份标识；

[0077] 接收单元，用于接收所述服务器发送的设备身份标识。

[0078] 在一些实施例中，其中发送单元，包括：

[0079] 加密模块，用于使用客户端预设的加密密钥加密所述设备身份标识，

[0080] 发送模块，用于将携带加密后的设备身份标识的密钥获取请求发送给服务器，以便服务器使用所述客户端预设的加密密钥所对应的解密密钥对加密后的设备身份标识进行解密，若解密成功，生成所述身份认证密钥。

[0081] 在一些实施例中，其中发送单元，还包括：

[0082] 签名模块，用于使用所述客户端预设的签名密钥签名生成签名信息；

[0083] 发送模块，还用于将携带签名信息的密钥获取请求发送给服务器，以便若解密成功，生成所述身份认证密钥之前，服务器使用所述客户端预设的验签密钥对所述签名信息进行验签，若验签通过，生成所述身份认证密钥。

[0084] 在一些实施例中，其中

[0085] 保存单元，具体用于接收并直接保存所述服务器发送的身份认证密钥；

[0086] 或者，

[0087] 保存单元，具体用于接收所述服务器发送的身份认证密钥后，向服务器发送密钥验证请求，所述密钥验证请求中携带设备身份标识、利用身份认证密钥加密后的验证信息，以使服务器查找与所述设备身份标识具有预绑定关系的身份认证密钥，并通过使用查找到的身份认证密钥对所述验证信息进行解密，来对所述客户端进行密钥验证，若密钥验证通过，修改所述身份认证密钥与所述设备身份标识的预绑定关系为绑定关系；接收所述服务器发送的密钥验证通过信息后，保存所述服务器发送的身份认证密钥。

[0088] 在一些实施例中，其中

[0089] 保存单元，具体用于利用预设的解密密钥对接收到的身份认证密钥进行解密后，对解密后的身份认证密钥进行保存。

[0090] 第七方面，本公开的实施例提供了一种身份认证的装置，所述装置包括：

[0091] 接收单元，用于接收客户端发送的经身份认证密钥加密后的客户端身份认证请求和设备身份标识，所述身份认证密钥由第一方面所述的方法生成；

[0092] 查找单元，用于查找所述设备身份标识对应的身份认证密钥；

[0093] 身份验证单元，用于通过使用查找到的身份认证密钥对所述加密后的客户端身份认证请求进行解密，来对所述客户端进行身份验证。

[0094] 第八方面，本公开的实施例提供了一种身份认证的装置，所述装置包括：

[0095] 获取单元，用于获取身份认证密钥，所述身份认证密钥由第二方面所述的方法生成；

[0096] 加密单元，用于使用所述身份认证密钥对客户端身份认证请求进行加密；

[0097] 发送单元，用于携带设备身份标识将加密后的客户端身份认证请求发送给服务器，以便所述服务器查找所述设备身份标识对应的身份认证密钥，并通过使用查找到的身份认证密钥对所述加密后的客户端身份认证请求进行解密，来对客户端进行身份验证。

[0098] 第九方面，本公开的实施例提供了一种存储介质，所述存储介质包括存储的程序，其中，在所述程序运行时控制所述存储介质所在设备执行第一方面所述的身份认证密钥的生成方法，或者，在所述程序运行时控制所述存储介质所在设备执行第二方面所述的身份认证密钥的生成方法。

[0099] 第十方面，本公开的实施例提供了一种存储介质，所述存储介质包括存储的程序，其中，在所述程序运行时控制所述存储介质所在设备执行第三方面或第四方面所述的身份认证的方法。

[0100] 第十一方面，本公开的实施例提供了一种身份认证密钥的生成装置，所述装置包括存储介质；及一个或者多个处理器，所述存储介质与所述处理器耦合，所述处理器被配置为执行所述存储介质中存储的程序指令；所述程序指令运行时执行第一方面所述的身份认证密钥的生成方法。

[0101] 第十二方面，本公开的实施例提供了一种身份认证密钥的生成装置，所述装置包括存储介质；及一个或者多个处理器，所述存储介质与所述处理器耦合，所述处理器被配置为执行所述存储介质中存储的程序指令；所述程序指令运行时执行第二方面所述的身份认证密钥的生成方法。

[0102] 第十三方面，本公开的实施例提供了一种身份认证的装置，所述装置包括存储介

质;及一个或者多个处理器,所述存储介质与所述处理器耦合,所述处理器被配置为执行所述存储介质中存储的程序指令;所述程序指令运行时执行第三方面的身份认证的方法。

[0103] 第十四方面,本公开的实施例提供了一种身份认证的装置,所述装置包括存储介质;及一个或者多个处理器,所述存储介质与所述处理器耦合,所述处理器被配置为执行所述存储介质中存储的程序指令;所述程序指令运行时执行第四方面的身份认证的方法。

[0104] 第十五方面,本公开的实施例提供了一种身份认证密钥的生成系统,包括:终端和服务器;

[0105] 所述服务器包括第十一方面所述的身份认证密钥的生成装置;

[0106] 所述终端包括第十二方面所述的身份认证密钥的生成装置。

[0107] 第十六方面,本公开的实施例提供了一种身份认证的系统,包括:终端和服务器;

[0108] 所述服务器包括第十三方面所述的身份认证的装置;

[0109] 所述终端包括第十四方面所述的身份认证的装置。

[0110] 第十七方面,本公开的实施例提供了一种车辆,包括:第六方面所述的身份认证密钥的生成装置。

[0111] 第十八方面,本公开的实施例提供了一种车辆,包括:第八方面所述的身份认证的装置。

[0112] 第十九方面,本公开的实施例提供了一种身份认证密钥的生成系统,包括:车辆和服务器;

[0113] 所述服务器包括第五方面所述的身份认证密钥的生成装置;

[0114] 所述车辆包括第六方面所述的身份认证密钥的生成装置。

[0115] 第二十方面,本公开的实施例提供了一种身份认证的系统,包括:车辆和服务器;

[0116] 所述服务器包括第七方面所述的身份认证密钥的生成装置;

[0117] 所述车辆包括第八方面所述的身份认证的装置。

[0118] 借由上述技术方案,本公开的实施例提供的身份认证密钥的生成方法、身份认证的方法、装置及系统至少具有下列优点:

[0119] 本公开的实施例提供的身份认证密钥的生成方法、身份认证的方法、装置及系统,根据客户端发送的携带有设备身份标识的密钥获取请求,为客户端建立用于认证客户端身份的身份认证密钥与设备身份标识的绑定关系,并将身份认证密钥发送至客户端,使客户端进行保存。相对于现有技术,软件厂商无需与终端设备的生产厂商合作,而是当用户在使用软件(客户端)时候,为客户端配属与客户端的设备身份标识绑定的身份认证密钥,可以使服务器通过查询与设备身份标识之间建立的绑定关系的身份认证密钥对客户端进行身份认证。

[0120] 上述说明仅是本公开的实施例技术方案的概述,为了能够更清楚了解本公开的实施例的技术手段,而可依照说明书的内容予以实施,并且为了让本公开的实施例的上述和其它目的、特征和优点能够更明显易懂,以下特举本公开的实施例的具体实施方式。

附图说明

[0121] 通过阅读下文优选实施方式的详细描述,各种其他的优点和益处对于本领域普通技术人员将变得清楚明了。附图仅用于示出优选实施方式的目的,而并不认为是对本公开

的实施例的限制。而且在整个附图中，用相同的参考符号表示相同的部件。在附图中：

[0122] 图1示出了本公开的第一方面实施例提供的一种身份认证密钥的生成方法的流程图；

[0123] 图2示出了本公开的第二方面实施例提供的一种身份认证密钥的生成方法的流程图；

[0124] 图3示出了本公开的第三方面实施例提供的一种身份认证密钥的生成方法的流程图；

[0125] 图4示出了本公开的第四方面实施例提供的一种身份认证密钥的生成方法的流程图；

[0126] 图5示出了本公开的第五方面实施例提供的一种身份认证密钥的生成方法的流程图；

[0127] 图6示出了本公开的第六方面实施例提供的一种身份认证的方法的流程图；

[0128] 图7示出了本公开的第七方面实施例提供的一种身份认证的方法的流程图；

[0129] 图8示出了本公开的第八方面实施例提供的一种身份认证密钥的生成装置的结构示意图；

[0130] 图9示出了本公开的第八方面实施例提供的一种具体的身份认证密钥的生成装置的结构示意图；

[0131] 图10示出了本公开的第九方面实施例提供的一种身份认证密钥的生成装置的结构示意图；

[0132] 图11示出了本公开的第九方面实施例提供的一种具体的身份认证密钥的生成装置的结构示意图；

[0133] 图12示出了本公开的第十方面实施例提供的一种身份认证的装置的结构示意图；

[0134] 图13示出了本公开的第十一方面实施例提供的一种身份认证的装置的结构示意图。

具体实施方式

[0135] 下面将参照附图更详细地描述本公开的示例性实施例。虽然附图中显示了本公开的示例性实施例，然而应当理解，可以以各种形式实现本公开而不应被这里阐述的实施例所限制。相反，提供这些实施例是为了能够更透彻地理解本公开，并且能够将本公开的范围完整的传达给本领域的技术人员。

[0136] 本公开的实施例提供了一种身份认证密钥的生成方法，可应用于为安装有客户端(应用程序)的终端和服务器之间配置用于身份认证的身份认证密钥。

[0137] 第一方面，如图1所示，本公开的实施例提供了一种身份认证密钥的生成方法，可应用于服务器一侧，服务器的执行动作可以为云端或者服务器端的服务，例如，可包括：应用程序编程接口API(Application Programming Interface，简写API)服务、加密服务、设备服务，但不局限于此。如图1所示，所述方法主要包括：

[0138] 101接收客户端发送的密钥获取请求，所述密钥获取请求中携带有设备身份标识；

[0139] 不同的服务器在实际的应用当中，接收密钥获取请求的方式可能会有所差异，可以有直接接收的情况，或是通过配置应用程序编程接口API服务来接收密钥获取请求。

[0140] 设备身份标识为与服务器身份认证数据交互的终端的身份标识，其可被实施为手机号、自定义账号、终端标识(如终端媒体访问控制地址MAC(Media Access Control Address，简写MAC))、生物特征(如声纹、虹膜)、随机分配标识中任一的一个或多个的组合等，本发明实施例中不做限定。

[0141] 102生成用于认证所述客户端身份的身份认证密钥；

[0142] 身份认证密钥可以包含有对称密钥、非对称密钥中的至少一种，密钥的个数不局限于一个或多个，例如，身份认证密钥可以包括信息加密密钥和信息签名密钥，也可以至包含信息加密密钥或信息签名密钥。对称密钥可采用对称加密算法生成，如数据加密标准(Data Encryption Standard，简写DES)加密算法、高级加密标准(Advanced Encryption Standard，简写AES)加密算法。非对称密钥采用非对称加密算法生成，如RSA加密算法等。

[0143] 在一些实施例中，生成的身份认证密钥实际为对应的设备身份标识配置的专属身份认证密钥，对应于不同的设备身份标识对应生成的专属身份认证密钥不同，保证对应不同的设备身份标识对应生成的专属身份认证密钥的唯一性，可以保证后续只能在唯一终端的客户端中向服务器实现设备身份标识的身份认证。

[0144] 103建立所述身份认证密钥与所述设备身份标识的绑定关系，并将所述身份认证密钥发送至所述客户端进行保存。

[0145] 绑定关系可以理解为一种关联映射关系，即身份认证密钥与设备身份标识建立映射关系，具体的建立形式，可采用建表关联等，但不局限于此。当身份认证密钥包含非对称密钥，可将私钥发送至客户端进行保存，或者将私钥和公钥同时发送至客户端进行保存。

[0146] 本公开的实施例中，根据客户端发送的携带有设备身份标识的密钥获取请求，为客户端建立用于认证客户端身份的身份认证密钥与设备身份标识的绑定关系，并将身份认证密钥发送至客户端，使客户端进行保存，相对于现有技术，软件厂商无需与终端设备的生产厂商合作，而是当用户在使用软件(客户端)时候，为客户端配属与客户端的设备身份标识绑定的身份认证密钥，可以使服务器通过查询与设备身份标识之间建立的绑定关系的身份认证密钥对客户端进行身份认证。

[0147] 第二方面，基于第一方面实施例提供的身份认证密钥的生成方法，本公开的实施例提供了一种身份认证密钥的生成方法，可应用于服务器一侧，服务器的执行动作可以为云端或者服务器端的服务，例如，可包括：API服务、加密服务、设备服务，但不局限于此。如图2所示，所述方法主要包括：

[0148] 201在接收到所述客户端发送的设备身份标识获取请求后，为所述客户端创建设备身份标识；

[0149] 设备身份标识为与服务器身份认证数据交互的终端的身份标识，其可被实施为手机号、自定义账号、终端标识(如MAC、生物特征(如声纹、虹膜)、随机分配标识中任一的一个或多个的组合等，本发明实施例中不做限定。

[0150] 对应的，设备身份标识获取请求的方式可具有多种形式，例如，设备身份标识获取请求中携带有用户录入的自定义账号、生物特征等。也可以携带有从终端中读取的数据，例如手机号、终端标识等。又或是设备身份标识获取请求中携带有随机申请标识的信息等。对应于不同的请求方式，为用户创建设备身份标识。

[0151] 202将所述设备身份标识发送给所述客户端，以完成为所述客户端创建设备身份

标识的服务。

[0152] 实施当中，在一些实施例中，为客户端创建设备身份标识的服务当中，还同时记录为所述客户端创建设备身份标识的服务的服务时间，记录的服务时间不限于接收客户端发送的设备身份标识获取请求的时间点或是将所述设备身份标识发送给所述客户端的时间点，可根据设置选取。

[0153] 203接收客户端发送的密钥获取请求，所述密钥获取请求中携带有设备身份标识；

[0154] 204验证密钥获取请求的有效性，若有效，生成用于认证所述客户端身份的身份认证密钥；

[0155] 有效性的验证中，可以包括有密钥获取请求的解密有效性验证、签名有效性验证、时间有效性验证、唯一有效性验证、格式有效性验证、重复获取有效性验证中的至少一种。

[0156] 解密有效性验证中，所述密钥获取请求中携带的设备身份标识是使用所述客户端预设的加密密钥加密后的设备身份标识，使用所述客户端预设的加密密钥所对应的解密密钥对加密后的设备身份标识进行解密，若解密成功，生成用于认证所述客户端身份的身份认证密钥。预设的加密密钥、解密密钥可以为预先配置的，预设的加密密钥配置于客户端的安装应用程序中，预设的解密密钥配置于服务器中，对应于不同的客户端，预设的加密密钥、解密密钥可以相同。预设的加密密钥、解密密钥可以为对称密钥，也可以为非对称密钥，如RSA加密密钥。

[0157] 签名有效性验证中，所述密钥获取请求中还携带使用所述客户端预设的签名密钥签名后的签名信息，签名密钥可以对所述客户端和所述客户端所属终端的基本参数信息进行签名，使用所述客户端预设的验签密钥对所述签名信息进行验签，若验签通过，生成用于认证所述客户端身份的身份认证密钥。预设的验签密钥为预先配置的，预设的验签密钥可配置于客户端的安装应用程序和服务器中，其可以采用对称密钥，采用对称加密算法生成，签名算法可采用哈希消息认证码(Hash-based Message Authentication Code，简写HAMC)加密算法。客户端的基本参数信息可以包括软件名称、版本等，终端的基本参数信息可以包括MAC、手机号等。

[0158] 时间有效性验证中，计算接收客户端发送的密钥获取请求的时间和为所述客户端创建设备身份标识的服务的服务时间的时间间隔，若时间间隔小于预设间隔时间，时效性验证通过，生成用于认证所述客户端身份的身份认证密钥。

[0159] 唯一有效性验证中，查询接收的所述密钥获取请求是否为所述设备身份标识对应发送的唯一密钥获取请求，若是，生成用于认证所述客户端身份的身份认证密钥。

[0160] 格式有效性验证中，验证接收的所述密钥获取请求的设备身份标识是否满足预设的格式要求，若满足，生成用于认证所述客户端身份的身份认证密钥。

[0161] 重复获取有效性验证中，查询服务器中是否存在有所述密钥获取请求的设备身份标识对应绑定关系的身份认证密钥，若不存在，验证通过，生成用于认证所述客户端身份的身份认证密钥。

[0162] 容易理解的是，上述的有效性验证的方法中可以单独采用一个方法验证，实施中，只需要满足一个验证条件即生成用于认证所述客户端身份的身份认证密钥。当采用至少2个方法验证中，需要同时满足所有的验证条件，即通过所有的验证后，生成用于认证所述客户端身份的身份认证密钥。

[0163] 以同时包含解密有效性验证、签名有效性验证为例：

[0164] 使用所述客户端预设的加密密钥所对应的解密密钥对加密后的设备身份标识进行解密；

[0165] 生成用于认证所述客户端身份的身份认证密钥包括：

[0166] 若解密成功，使用所述客户端预设的验签密钥对所述签名信息进行验签；

[0167] 若验签通过，则生成所述身份认证密钥。

[0168] 其中，可以理解的，解密和验签的步骤实际中是根据服务器与客户端的身份认证的协议而定的，并不局限于上述的顺序。

[0169] 205建立所述身份认证密钥与所述设备身份标识的绑定关系，并将所述身份认证密钥发送至所述客户端进行保存。

[0170] 建立所述身份认证密钥与所述设备身份标识的绑定关系的过程，可以采用直接建立的方式。但是，直接建立绑定关系的方式存在缺点，当客户端与服务器之间的通信故障、或是客户端自身故障等问题下，导致客户端并未实际接收并保存身份认证密钥的情况下，由于客户端并未保存身份认证密钥，导致服务器建立了无效的身份认证密钥与所述设备身份标识的绑定关系。为了解决上述问题，建立所述身份认证密钥与所述设备身份标识的绑定关系，可包括：

[0171] 建立所述身份认证密钥与所述设备身份标识的预绑定关系，并将预绑定的身份认证密钥发送至所述客户端；其中，发送至所述客户端的预绑定的身份认证密钥可以使用所述客户端中预设的加密密钥对所述身份认证密钥加密，以便所述客户端利用预设的解密密钥对接收到的身份认证密钥进行解密；

[0172] 接收所述客户端发送的密钥验证请求，所述密钥验证请求中携带设备身份标识、利用身份认证密钥加密后的验证信息；

[0173] 查找与所述设备身份标识预绑定关系对应的身份认证密钥，并通过使用查找到的身份认证密钥对所述验证信息进行解密，来对所述客户端进行密钥验证，若密钥验证通过，修改所述身份认证密钥与所述设备身份标识的预绑定关系为绑定关系。

[0174] 其中，查找与所述设备身份标识预绑定关系对应的身份认证密钥之前，可进行验证密钥验证请求的有效性，若有效，查找与所述设备身份标识预绑定关系对应的身份认证密钥；

[0175] 密钥验证请求的有效性可以包括有密钥验证请求的时间有效性验证。

[0176] 密钥验证请求的时间有效性验证中，可以验证接收所述客户端发送的密钥验证请求的时间和密钥获取请求的时间有效性验证的时间的时间间隔，若时间间隔小于预设间隔时间，查找与所述设备身份标识预绑定关系对应的身份认证密钥。容易理解的是，密钥验证请求的时间有效性验证实际中为一个时间上的验证方法，其具体算法可以多样的变换，例如，可以验证接收所述客户端发送的密钥验证请求的时间和接收客户端发送的密钥获取请求的时间的时间间隔，若时间间隔小于预设间隔时间，查找与所述设备身份标识预绑定关系对应的身份认证密钥。

[0177] 在一些实施例中，在将所述身份认证密钥发送至所述客户端进行保存的步骤中，具体为：

[0178] 使用所述客户端中预设的加密密钥对所述身份认证密钥加密后发送至客户端，以

便所述客户端利用预设的解密密钥对接收到的身份认证密钥进行解密后，对解密后的身份认证密钥进行保存。将加密后的身份认证密钥发送至客户端，可以一定程度上提高身份认证密钥的保密性。

[0179] 第三方面，本公开的实施例提供了一种身份认证密钥的生成方法，可应用于客户端一侧，如图3所示，所述方法主要包括：

[0180] 301将密钥获取请求发送给服务器，以便所述服务器生成用于认证客户端身份的身份认证密钥，并建立所述身份认证密钥与所述密钥获取请求中携带的设备身份标识的绑定关系；

[0181] 不同的服务器在实际的应用当中，发送密钥获取请求的请求可能会有所差异，可以有直接发送设备服务的情况，或是通过配置应用程序编程接口API服务将密钥获取请求发送至设备服务。

[0182] 302接收并保存所述服务器发送的身份认证密钥。

[0183] 本公开的实施例中，通过向服务器发送的密钥获取请求，使服务器为客户端建立用于认证客户端身份的身份认证密钥与设备身份标识的绑定关系，并将身份认证密钥发送至客户端，从而接收并保存服务器发送的身份认证密钥，相对于现有技术，软件厂商无需与终端设备的生产厂商合作，而是当用户在使用软件(客户端)时候，为客户端配属与客户端的设备身份标识绑定的身份认证密钥，可以使客户端使用保存的身份认证密钥向服务器进行身份认证。

[0184] 第四方面，基于第三方面实施例提供的身份认证密钥的生成方法，本公开的实施例提供了一种身份认证密钥的生成方法，可应用于客户端一侧，如图4所示，所述方法主要包括：

[0185] 401将设备身份标识获取请求发送给服务器，以便所述服务器创建设备身份标识；

[0186] 对应的，设备身份标识获取请求的方式可具有多种形式，例如，设备身份标识获取请求中携带有用户录入的自定义账号、生物特征等。也可以携带有从终端中读取的数据，例如手机号、终端标识等。又或是设备身份标识获取请求中携带有随机申请标识的信息等。对应于不同的请求方式，创建的设备身份标识可以根据设备身份标识获取请求的方式而定，例如，根据用户录入的自定义账号、生物特征、从终端中读取的数据、随机申请标识等创建设备身份标识，但不局限于此。

[0187] 402接收所述服务器发送的设备身份标识；

[0188] 403将密钥获取请求发送给服务器，以便所述服务器生成用于认证客户端身份的身份认证密钥，并建立所述身份认证密钥与所述密钥获取请求中携带的设备身份标识的绑定关系；

[0189] 在一些实施例中，其中，密钥获取请求中可携带加密后的设备身份标识，将密钥获取请求发送给服务器，以便所述服务器生成用于认证客户端身份的身份认证密钥，具体为：使用客户端预设的加密密钥加密所述设备身份标识；将携带加密后的设备身份标识的密钥获取请求发送给服务器，以便服务器使用所述客户端预设的加密密钥所对应的解密密钥对加密后的设备身份标识进行解密，若解密成功，生成所述身份认证密钥。

[0190] 在一些实施例中，其中，密钥获取请求中可携带签名信息，将密钥获取请求发送给服务器，以便所述服务器生成用于认证客户端身份的身份认证密钥，具体为：使用所述客户

端预设的签名密钥签名生成签名信息;将携带签名信息的密钥获取请求发送给服务器,以便服务器使用所述客户端预设的验签密钥对所述签名信息进行验签,若验签通过,生成所述身份认证密钥。

[0191] 在一些实施例中,其中,密钥获取请求中可同时携带加密后的设备身份标识和签名信息,将密钥获取请求发送给服务器,以便所述服务器生成用于认证客户端身份的身份认证密钥,具体为:

[0192] 使用客户端预设的加密密钥加密所述设备身份标识;

[0193] 使用所述客户端预设的签名密钥签名生成签名信息;

[0194] 将携带签名信息、携带加密后的设备身份标识的密钥获取请求发送给服务器,以便服务器使用所述客户端预设的加密密钥所对应的解密密钥对加密后的设备身份标识进行解密,若解密成功,服务器使用所述客户端预设的验签密钥对所述签名信息进行验签,若验签通过,生成所述身份认证密钥。

[0195] 或是,

[0196] 使用客户端预设的加密密钥加密所述设备身份标识;

[0197] 使用所述客户端预设的签名密钥签名生成签名信息;

[0198] 将携带签名信息、携带加密后的设备身份标识的密钥获取请求发送给服务器,以便服务器使用所述客户端预设的验签密钥对所述签名信息进行验签,若验签通过,服务器使用所述客户端预设的加密密钥所对应的解密密钥对加密后的设备身份标识进行解密,若解密成功,生成所述身份认证密钥。

[0199] 具体的流程顺序可以根据预定的身份认证协议而定。

[0200] 404接收并保存所述服务器发送的身份认证密钥。

[0201] 保存身份认证密钥的过程,可以采用直接保存的方式。但是,直接保存的方式存在缺点,当客户端与服务器之间的通信故障、或是客户端自身故障等问题下,导致客户端并未实际接收并保存身份认证密钥的情况下,由于客户端并未保存身份认证密钥,导致服务器建立了无效的身份认证密钥与所述设备身份标识的绑定关系。为了解决上述问题,接收并保存所述服务器发送的身份认证密钥,可包括:

[0202] 接收所述服务器发送的身份认证密钥后,向服务器发送密钥验证请求,所述密钥验证请求中携带设备身份标识、利用身份认证密钥加密后的验证信息,以使服务器查找与所述设备身份标识具有预绑定关系的身份认证密钥,并通过使用查找到的身份认证密钥对所述验证信息进行解密,来对所述客户端进行密钥验证,若密钥验证通过,修改所述身份认证密钥与所述设备身份标识的预绑定关系为绑定关系;

[0203] 接收所述服务器发送的密钥验证通过信息后,保存所述服务器发送的身份认证密钥。

[0204] 在一些实施例中,服务器将加密后的身份认证密钥发送至客户端,接收并保存所述服务器发送的身份认证密钥,具体为:

[0205] 利用预设的解密密钥对接收到的身份认证密钥进行解密后,对解密后的身份认证密钥进行保存。

[0206] 第五方面,基于上述四个方面实施例提供的身份认证密钥的生成方法,本公开的实施例提供了一种身份认证密钥的生成方法,应用于客户端和服务器之间的交互,服务器

的执行动作可以为云端或者服务器端的服务，例如，可包括：API服务、加密服务、设备服务，但不局限于此。如图5所示，所述方法主要包括：

[0207] 501对于未注册的客户端，将设备身份标识获取请求发送给服务器，服务器在接收到所述客户端发送的设备身份标识获取请求后，为所述客户端创建设备身份标识，并记录为所述客户端创建设备身份标识的服务的服务时间；

[0208] 502服务器将所述设备身份标识发送给所述客户端，以完成为所述客户端创建设备身份标识的服务。

[0209] 503客户端使用客户端预设的加密密钥加密所述设备身份标识；

[0210] 504客户端使用客户端预设的签名密钥签名生成签名信息；

[0211] 505将携带加密后的设备身份标识、签名密钥的密钥获取请求发送给服务器；

[0212] 506API服务对密钥获取请求的时间有效性验证、唯一有效性验证；

[0213] 507加密服务对密钥获取请求签名有效性验证；

[0214] 508设备服务对密钥获取请求格式有效性验证、重复获取有效性验证；

[0215] 509设备服务对密钥获取请求解密有效性验证；

[0216] 510若解密有效性验证、签名有效性验证、时间有效性验证、唯一有效性验证、格式有效性验证、重复获取有效性验证通过，生成用于认证所述客户端身份的身份认证密钥；

[0217] 511建立所述身份认证密钥与所述设备身份标识的预绑定关系；

[0218] 512使用所述客户端中预设的加密密钥对所述身份认证密钥加密；其中，客户端中预设的加密密钥可预先存储于服务器，其可以为对称密钥，实施中存储于客户端和服务器的预设密钥也可以为非对称密钥；

[0219] 513加密服务使用预先存储于服务器中预设的加密密钥生成服务器的签名信息；

[0220] 514API服务将服务器的签名信息、加密的身份认证密钥发送至客户端；

[0221] 515客户端利用预设的解密密钥对接收到的签名信息进行验签；

[0222] 516客户端利用预设的解密密钥对接收到的身份认证密钥进行解密；

[0223] 517若验签、解密通过，客户端向服务器发送密钥验证请求，所述密钥验证请求中携带设备身份标识、利用身份认证密钥加密后的验证信息以及客户端签名；

[0224] 518加密服务使用存储于服务器的身份认证密钥对客户端签名验签；

[0225] 519设备服务对密钥验证请求的时间有效性验证；

[0226] 520若签名验证、时间有效性验证通过，查找与所述设备身份标识预绑定关系对应的身份认证密钥，并通过使用查找到的身份认证密钥对所述验证信息进行解密，来对所述客户端进行密钥验证；

[0227] 521若密钥验证通过，修改所述身份认证密钥与所述设备身份标识的预绑定关系为绑定关系；

[0228] 522使用服务器预设的密钥对身份认证密钥加密；

[0229] 523使用服务器预设的密钥生成服务器签名信息；

[0230] 524API服务将服务器的签名信息、加密的身份认证密钥再次发送至客户端；

[0231] 525客户端利用预设的解密密钥对接收到的签名信息进行验签；

[0232] 526客户端利用预设的解密密钥对接收到的身份认证密钥进行解密；

[0233] 527若验签、解密通过，客户端保存身份认证密钥。

[0234] 本公开的实施例提供了一种身份认证的方法，可应用于为安装有客户端(应用程序)的终端和服务器之间进行身份认证。

[0235] 第六方面，本公开的实施例提供了一种身份认证的方法，可应用于服务器一侧，服务器的执行动作可以为云端或者服务器端的服务，例如，可包括：应用程序编程接口API服务、加密服务、设备服务，但不局限于此。如图6所示，所述方法主要包括：

[0236] 601接收客户端发送的经身份认证密钥加密后的客户端身份认证请求和设备身份标识，所述身份认证密钥的生成方法包括：接收客户端发送的密钥获取请求，所述密钥获取请求中携带有设备身份标识；生成用于认证所述客户端身份的身份认证密钥；建立所述身份认证密钥与所述设备身份标识的绑定关系，并将所述身份认证密钥发送至所述客户端进行保存；

[0237] 602查找所述设备身份标识对应的身份认证密钥；

[0238] 其中，服务器中预先存于有与设备身份标识绑定的身份认证密钥，即为与设备身份标识对应的身份认证密钥。

[0239] 603并通过使用查找到的身份认证密钥对所述加密后的客户端身份认证请求进行解密，来对所述客户端进行身份验证。

[0240] 当身份认证密钥采用对称密钥时，身份认证的解密方法可采用对称加密算法，如DES加密算法、AES加密算法，客户端的身份认证请求使用身份认证密钥采用对称加密算法加密后发送给服务器，服务器使用身份认证密钥对加密的身份认证请求进行解密后认证判断，来对用户进行身份认证。当采用非对称密钥时，身份认证的方法可采用非对称加密算法，如RSA加密算法，客户端的身份认证请求使用身份认证密钥(私钥)采用非对称加密算法加密后发送给服务器，服务器使用身份认证密钥(公钥)对加密的身份认证请求进行解密后认证判断，来对用户进行身份认证。

[0241] 身份认证密钥的生成方法具体可参见上述的第一方面或第二方面的身份认证密钥的生成方法，本实施例中不再赘述。

[0242] 第七方面，本公开的实施例提供了一种身份认证的方法，可应用于客户端一侧，如图7所示，所述方法主要包括：

[0243] 701获取身份认证密钥，所述身份认证密钥的生成方法包括：将密钥获取请求发送给服务器，以便所述服务器生成用于认证客户端身份的身份认证密钥，并建立所述身份认证密钥与所述密钥获取请求中携带的设备身份标识的绑定关系；接收并保存所述服务器发送的身份认证密钥。

[0244] 702使用所述身份认证密钥对客户端身份认证请求进行加密；

[0245] 703携带设备身份标识将加密后的客户端身份认证请求发送给服务器，以便所述服务器查找所述设备身份标识对应的身份认证密钥，并通过使用查找到的身份认证密钥对所述加密后的客户端身份认证请求进行解密，来对客户端进行身份验证。

[0246] 身份认证密钥的生成方法具体可参见上述的第三方面或第四方面的身份认证密钥的生成方法，本实施例中不再赘述。

[0247] 基于同一发明技术构思，第八方面，依据图1或图2所示的方法，本公开的另一个实施例还提供了一种身份认证密钥的生成装置，如图8所示，所述装置主要包括：

[0248] 接收单元810，用于接收客户端发送的密钥获取请求，所述密钥获取请求中携带有

设备身份标识；

[0249] 生成单元820，用于生成用于认证所述客户端身份的身份认证密钥；

[0250] 建立单元830，用于建立所述身份认证密钥与所述设备身份标识的绑定关系，

[0251] 发送单元840，用于将所述身份认证密钥发送至所述客户端进行保存。

[0252] 在一些实施例中，如图9所示，其中还包括：

[0253] 创建单元850，用于在接收客户端发送的密钥获取请求之前，在接收到所述客户端发送的设备身份标识获取请求后，为所述客户端创建设备身份标识；

[0254] 发送单元840，用于将所述设备身份标识发送给所述客户端。

[0255] 在一些实施例中，其中还包括：

[0256] 解密单元860，用于当所述密钥获取请求中携带的设备身份标识是使用所述客户端预设的加密密钥加密后的设备身份标识时，在生成用于认证所述客户端身份的身份认证密钥之前，使用所述客户端预设的加密密钥所对应的解密密钥对加密后的设备身份标识进行解密；

[0257] 生成单元820具体用于若解密成功，则生成所述身份认证密钥。

[0258] 在一些实施例中，其中还包括：

[0259] 验签单元870，用于当所述密钥获取请求中还携带使用所述客户端预设的签名密钥签名后的签名信息时，若解密成功，则在生成所述身份认证密钥之前，使用所述客户端预设的验签密钥对所述签名信息进行验签；

[0260] 生成单元820具体用于若验签通过，则生成所述身份认证密钥。

[0261] 在一些实施例中，其中

[0262] 建立单元830具体用于直接建立所述身份认证密钥与所述设备身份标识的绑定关系；

[0263] 或者，

[0264] 建立单元830具体用于建立所述身份认证密钥与所述设备身份标识的预绑定关系，并将预绑定的身份认证密钥发送至所述客户端，接收所述客户端发送的密钥验证请求，所述密钥验证请求中携带设备身份标识、利用身份认证密钥加密后的验证信息，查找与所述设备身份标识预绑定关系对应的身份认证密钥，并通过使用查找到的身份认证密钥对所述验证信息进行解密，来对所述客户端进行密钥验证，若密钥验证通过，修改所述身份认证密钥与所述设备身份标识的预绑定关系为绑定关系。

[0265] 在一些实施例中，其中

[0266] 建立单元830具体用于使用所述客户端中预设的加密密钥对所述身份认证密钥加密后发送至客户端，以便所述客户端利用预设的解密密钥对接收到的身份认证密钥进行解密后，对解密后的身份认证密钥进行保存。

[0267] 第八方面的实施例提供的身份认证密钥的生成装置，可以用以执行第一方面或第二方面的实施例所提供的身份认证密钥的生成方法，相关的用于的含义以及具体的实施方式可以参见第一方面或第二方面的实施例中的相关描述，在此不再详细说明。

[0268] 基于同一发明技术构思，第九方面，依据图3或图4所示的方法，本公开的另一个实施例还提供了一种身份认证密钥的生成装置，如图10所示，所述装置主要包括：

[0269] 发送单元910，用于将密钥获取请求发送给服务器，以便所述服务器生成用于认证

客户端身份的身份认证密钥，并建立所述身份认证密钥与所述密钥获取请求中携带的设备身份标识的绑定关系；

[0270] 保存单元920，用于接收并保存所述服务器发送的身份认证密钥。

[0271] 在一些实施例中，如图11所示，其中还包括：

[0272] 发送单元910，用于在将密钥获取请求发送给服务器之前，将设备身份标识获取请求发送给服务器，以便所述服务器创建设备身份标识；

[0273] 接收单元930，用于接收所述服务器发送的设备身份标识。

[0274] 在一些实施例中，其中发送单元910，包括：

[0275] 加密模块911，用于使用客户端预设的加密密钥加密所述设备身份标识，

[0276] 发送模块912，用于将携带加密后的设备身份标识的密钥获取请求发送给服务器，以便服务器使用所述客户端预设的加密密钥所对应的解密密钥对加密后的设备身份标识进行解密，若解密成功，生成所述身份认证密钥。

[0277] 在一些实施例中，其中发送单元910，还包括：

[0278] 签名模块913，用于使用所述客户端预设的签名密钥签名生成签名信息；

[0279] 发送模块912，还用于将携带签名信息的密钥获取请求发送给服务器，以便若解密成功，生成所述身份认证密钥之前，服务器使用所述客户端预设的验签密钥对所述签名信息进行验签，若验签通过，生成所述身份认证密钥。

[0280] 在一些实施例中，其中

[0281] 保存单元920，具体用于接收并直接保存所述服务器发送的身份认证密钥；

[0282] 或者，

[0283] 保存单元920，具体用于接收所述服务器发送的身份认证密钥后，向服务器发送密钥验证请求，所述密钥验证请求中携带设备身份标识、利用身份认证密钥加密后的验证信息，以使服务器查找与所述设备身份标识具有预绑定关系的身份认证密钥，并通过使用查找到的身份认证密钥对所述验证信息进行解密，来对所述客户端进行密钥验证，若密钥验证通过，修改所述身份认证密钥与所述设备身份标识的预绑定关系为绑定关系；接收所述服务器发送的密钥验证通过信息后，保存所述服务器发送的身份认证密钥。

[0284] 在一些实施例中，其中

[0285] 保存单元920，具体用于利用预设的解密密钥对接收到的身份认证密钥进行解密后，对解密后的身份认证密钥进行保存。

[0286] 第九方面的实施例提供的身份认证密钥的生成装置，可以用以执行第三方面或第四方面的实施例所提供的身份认证密钥的生成方法，相关的用于的含义以及具体的实施方式可以参见第三方面或第四方面的实施例中的相关描述，在此不再详细说明。

[0287] 第十方面，如图12所示，本公开的实施例提供了一种身份认证的装置，所述装置包括：

[0288] 接收单元111，用于接收客户端发送的经身份认证密钥加密后的客户端身份认证请求和设备身份标识，所述身份认证密钥由第一方面或第二方面所述的方法生成；

[0289] 查找单元112，用于查找所述设备身份标识对应的身份认证密钥；

[0290] 身份验证单元113，用于通过使用查找到的身份认证密钥对所述加密后的客户端身份认证请求进行解密，来对所述客户端进行身份验证。

[0291] 第十一方面，如图13所示，本公开的实施例提供了一种身份认证的装置，所述装置包括：

[0292] 获取单元121，用于获取身份认证密钥，所述身份认证密钥由第三方面或第四方面所述的方法生成；

[0293] 加密单元122，用于使用所述身份认证密钥对客户端身份认证请求进行加密；

[0294] 发送单元123，用于携带设备身份标识将加密后的客户端身份认证请求发送给服务器，以便所述服务器查找所述设备身份标识对应的身份认证密钥，并通过使用查找到的身份认证密钥对所述加密后的客户端身份认证请求进行解密，来对客户端进行身份验证。

[0295] 第十二方面，本公开的实施例提供了一种存储介质，所述存储介质包括存储的程序，其中，在所述程序运行时控制所述存储介质所在设备执行第一方面或第二方面或第四方面或第五方面所述的身份认证密钥的生成方法。

[0296] 存储介质可能包括计算机可读介质中的非永久性存储器，随机存取存储器(RAM)和/或非易失性内存等形式，如只读存储器(ROM)或闪存(flash RAM)，存储器包括至少一个存储芯片。

[0297] 第十三方面，本公开的实施例提供了一种存储介质，所述存储介质包括存储的程序，其中，在所述程序运行时控制所述存储介质所在设备执行第一方面或第二方面或第四方面或第五方面所述的身份认证的方法。

[0298] 存储介质可能包括计算机可读介质中的非永久性存储器，随机存取存储器(RAM)和/或非易失性内存等形式，如只读存储器(ROM)或闪存(flash RAM)，存储器包括至少一个存储芯片。

[0299] 第十四方面，本公开的实施例提供了一种身份认证密钥的生成装置，所述装置包括存储介质；及一个或者多个处理器，所述存储介质与所述处理器耦合，所述处理器被配置为执行所述存储介质中存储的程序指令；所述程序指令运行时执行第一方面或第二方面所述的身份认证密钥的生成方法。

[0300] 第十五方面，本公开的实施例提供了一种身份认证密钥的生成装置，所述装置包括存储介质；及一个或者多个处理器，所述存储介质与所述处理器耦合，所述处理器被配置为执行所述存储介质中存储的程序指令；所述程序指令运行时执行第三方面或第四方面所述的身份认证密钥的生成方法。

[0301] 第十六方面，本公开的实施例提供了一种身份认证的装置，所述装置包括存储介质；及一个或者多个处理器，所述存储介质与所述处理器耦合，所述处理器被配置为执行所述存储介质中存储的程序指令；所述程序指令运行时执行第五方面所述的身份认证方法。

[0302] 第十七方面，本公开的实施例提供了一种身份认证的装置，所述装置包括存储介质；及一个或者多个处理器，所述存储介质与所述处理器耦合，所述处理器被配置为执行所述存储介质中存储的程序指令；所述程序指令运行时执行第六方面所述的身份认证方法。

[0303] 第十八方面，本公开的实施例提供了一种身份认证密钥的生成系统，包括：终端和服务器；所述服务器包括第十四方面所述的身份认证密钥的生成装置；所述终端包括第十五方面所述的身份认证密钥的生成装置。

[0304] 第十九方面，本公开的实施例提供了一种身份认证的系统，包括：终端和服务器；所述服务器包括第十六方面所述的身份认证密钥的生成装置；所述终端包括第十七方面所

述的身份认证密钥的生成装置。

[0305] 第二十方面，本公开的实施例提供了一种车辆，包括：具体实施方式中第九方面所述的身份认证密钥的生成装置。

[0306] 第二十一方面，本公开的实施例提供了一种车辆，包括：具体实施方式中第十一方面所述的身份认证的装置。

[0307] 第二十二方面，本公开的实施例提供了一种身份认证密钥的生成系统，包括：车辆和服务器；

[0308] 所述服务器包括具体实施方式中第八方面所述的身份认证密钥的生成装置；

[0309] 所述车辆包括具体实施方式中第九方面所述的身份认证密钥的生成装置。

[0310] 第二十三方面，本公开的实施例提供了一种身份认证的系统，包括：车辆和服务器；

[0311] 所述服务器包括具体实施方式中第十方面所述的身份认证密钥的生成装置；

[0312] 所述车辆包括具体实施方式中第十一方面所述的身份认证的装置。

[0313] 本领域内的技术人员应明白，本公开的实施例可提供为方法、系统、或计算机程序产品。因此，本公开的实施例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，本公开的实施例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。

[0314] 本申请是参照本公开的实施例的方法、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装置。

[0315] 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。

[0316] 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。

[0317] 在一个典型的配置中，计算设备包括一个或多个处理器(CPU)、输入/输出接口、网络接口和内存。

[0318] 存储器可能包括计算机可读介质中的非永久性存储器，随机存取存储器(RAM)和/或非易失性内存等形式，如只读存储器(ROM)或闪存(flash RAM)。存储器是计算机可读介质的示例。

[0319] 计算机可读介质包括永久性和非永久性、可移动和非可移动媒体可以由任何方法或技术来实现信息存储。信息可以是计算机可读指令、数据结构、程序的模块或其他数据。

计算机的存储介质的例子包括,但不限于相变内存(PRAM)、静态随机存取存储器(SRAM)、动态随机存取存储器(DRAM)、其他类型的随机存取存储器(RAM)、只读存储器(ROM)、电可擦除可编程只读存储器(EEPROM)、快闪记忆体或其他内存技术、只读光盘只读存储器(CD-ROM)、数字多功能光盘(DVD)或其他光学存储、磁盒式磁带,磁带磁磁盘存储或其他磁性存储设备或任何其他非传输介质,可用于存储可以被计算设备访问的信息。按照本文中的界定,计算机可读介质不包括暂存电脑可读媒体(transitory media),如调制的数据信号和载波。

[0320] 还需要说明的是,术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含,从而使得包括一系列要素的过程、方法、商品或者设备不仅包括那些要素,而且还包括没有明确列出的其他要素,或者是还包括为这种过程、方法、商品或者设备所固有的要素。在没有更多限制的情况下,由语句“包括一个……”限定的要素,并不排除在包括要素的过程、方法、商品或者设备中还存在另外的相同要素。

[0321] 本领域技术人员应明白,本公开的实施例可提供为方法、系统或计算机程序产品。因此,本公开的实施例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,本公开的实施例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。

[0322] 以上仅为本申请的实施例而已,并不用于限制本申请。对于本领域技术人员来说,本申请可以有各种更改和变化。凡在本申请的精神和原理之内所作的任何修改、等同替换、改进等,均应包含在本申请的权利要求范围之内。

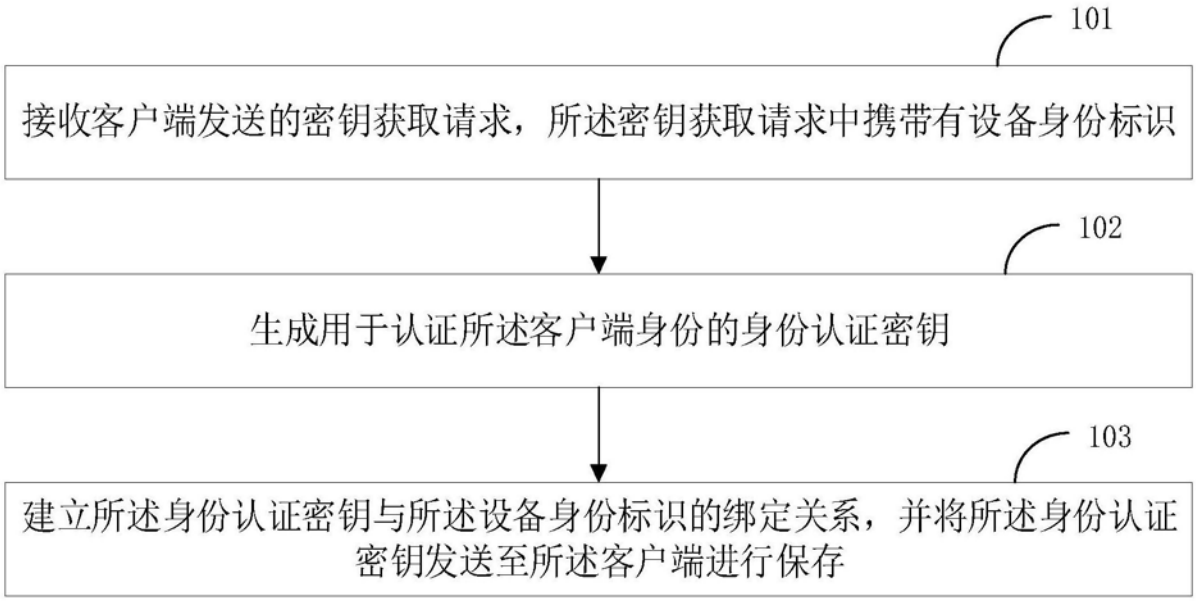

101
接收客户端发送的密钥获取请求，所述密钥获取请求中携带有设备身份标识
102
生成用于认证所述客户端身份的身份认证密钥
103
建立所述身份认证密钥与所述设备身份标识的绑定关系，并将所述身份认证密钥发送至所述客户端进行保存

图1

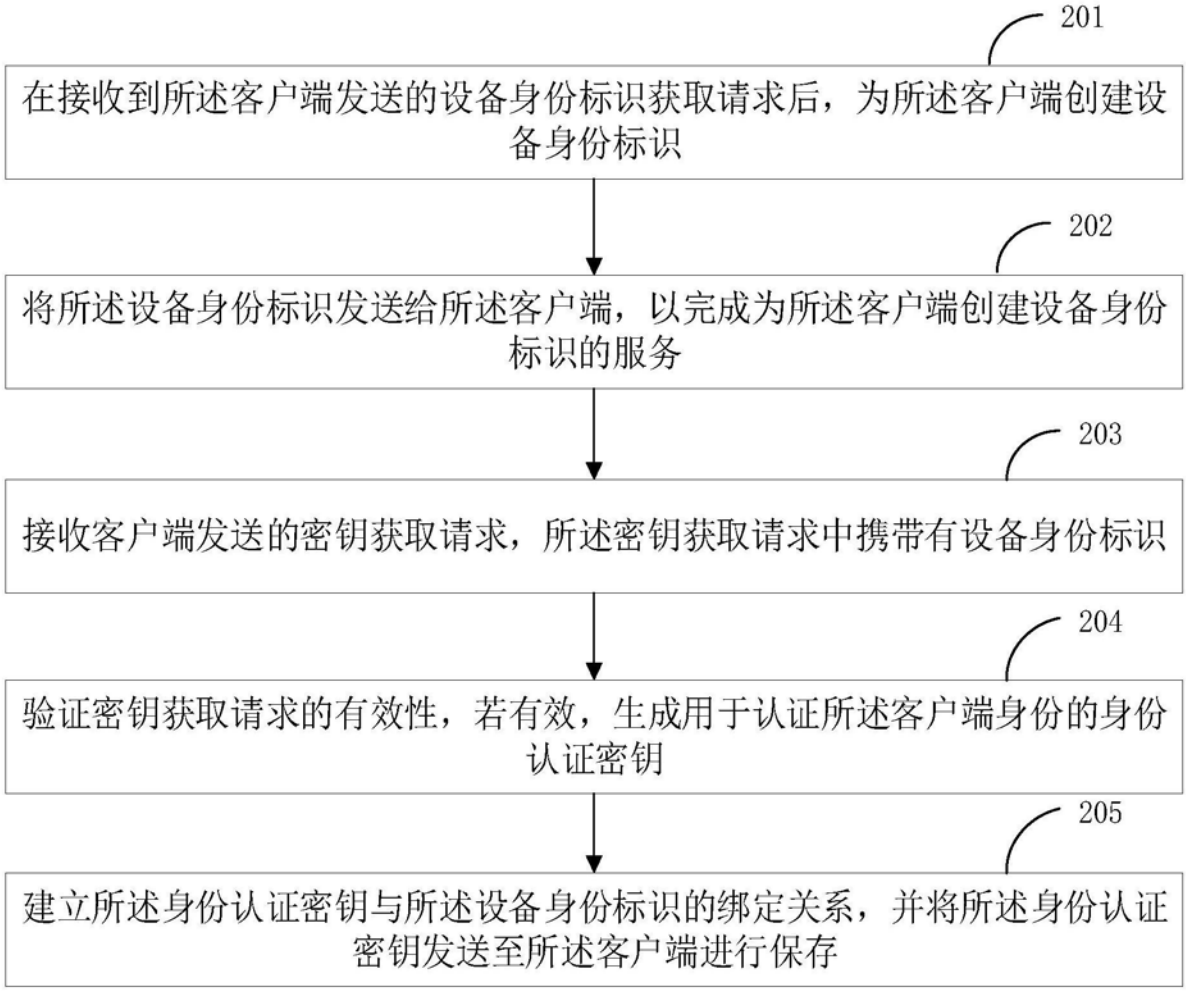

201
在接收到所述客户端发送的设备身份标识获取请求后，为所述客户端创建设备身份标识
202
将所述设备身份标识发送给所述客户端，以完成为所述客户端创建设备身份标识的服务
203
接收客户端发送的密钥获取请求，所述密钥获取请求中携带有设备身份标识
204
验证密钥获取请求的有效性，若有效，生成用于认证所述客户端身份的身份认证密钥
205
建立所述身份认证密钥与所述设备身份标识的绑定关系，并将所述身份认证密钥发送至所述客户端进行保存

图2


301
将密钥获取请求发送给服务器，以便所述服务器生成用于认证客户端身份的身份认证密钥，并建立所述身份认证密钥与所述密钥获取请求中携带的设备身份标识的绑定关系
302
接收并保存所述服务器发送的身份认证密钥

图3

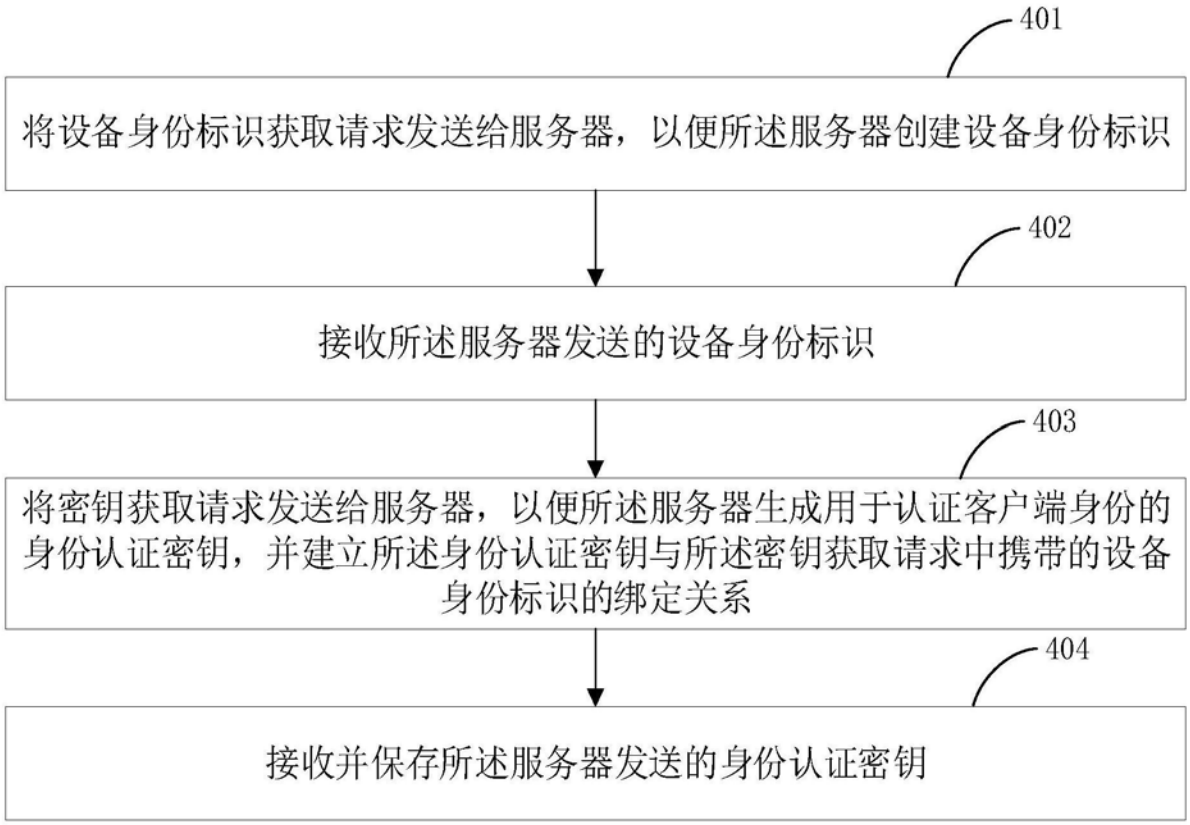

401
将设备身份标识获取请求发送给服务器，以便所述服务器创建设备身份标识
402
接收所述服务器发送的设备身份标识
403
将密钥获取请求发送给服务器，以便所述服务器生成用于认证客户端身份的身份认证密钥，并建立所述身份认证密钥与所述密钥获取请求中携带的设备身份标识的绑定关系
404
接收并保存所述服务器发送的身份认证密钥

图4

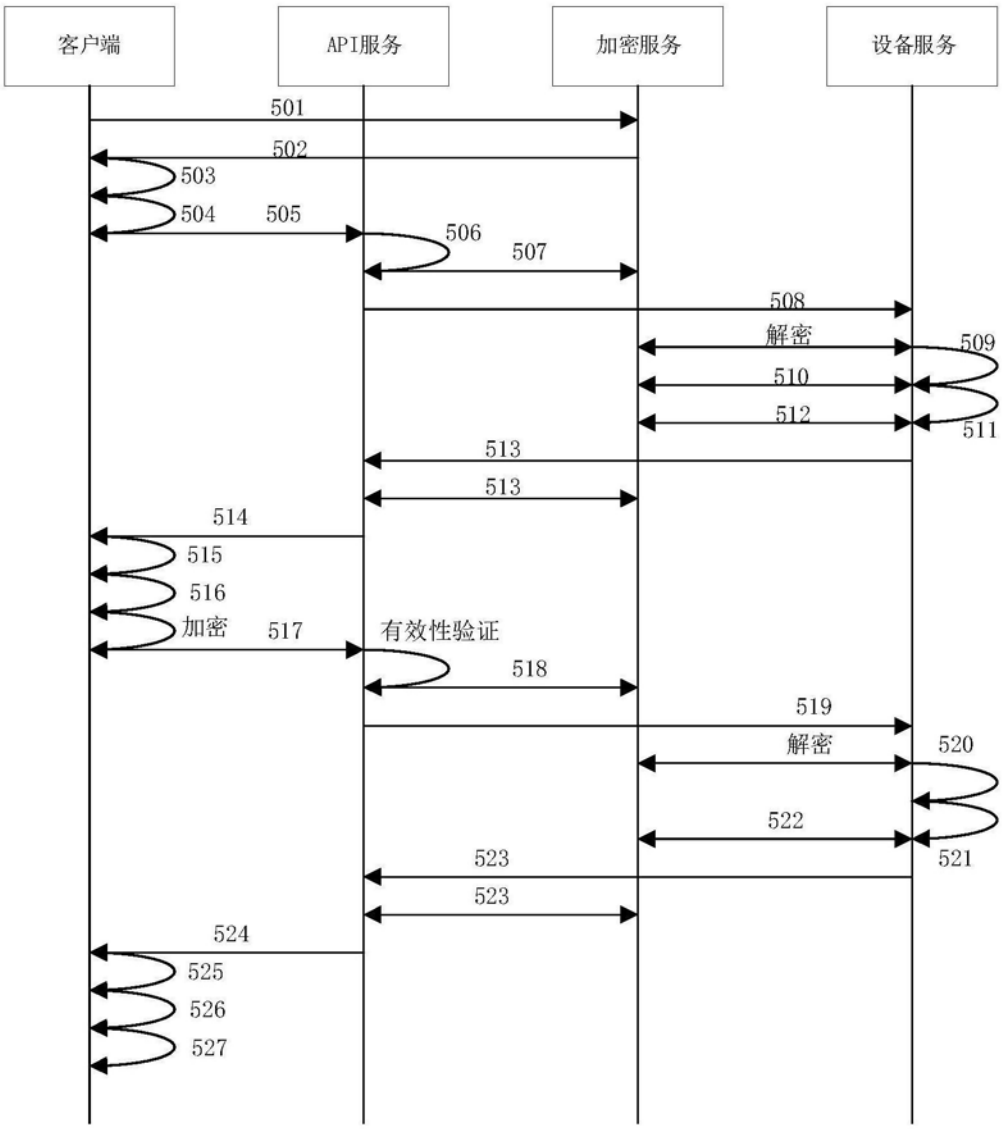

客户端
API服务
加密服务
设备服务
501
502
503
504
505
506
507
508
解密
509
510
512
511
513
513
514
515
516
加密
517
有效性验证
518
519
解密
520
522
521
523
523
524
525
526
527

图5

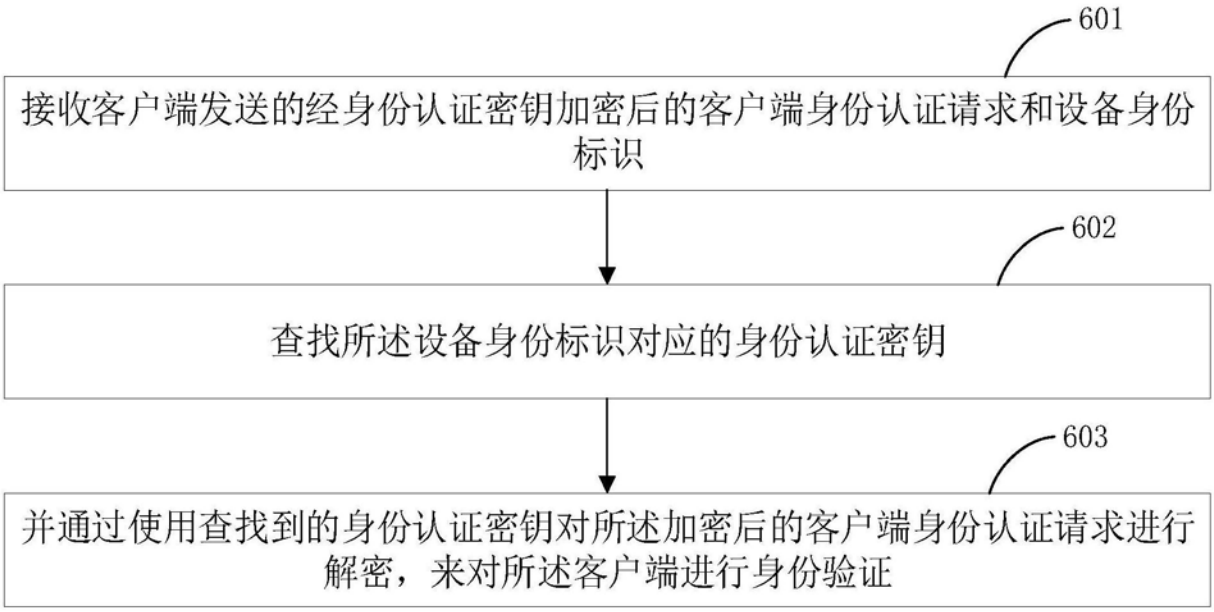

601
接收客户端发送的经身份认证密钥加密后的客户端身份认证请求和设备身份标识
602
查找所述设备身份标识对应的身份认证密钥
603
并通过使用查找到的身份认证密钥对所述加密后的客户端身份认证请求进行解密，来对所述客户端进行身份验证

图6

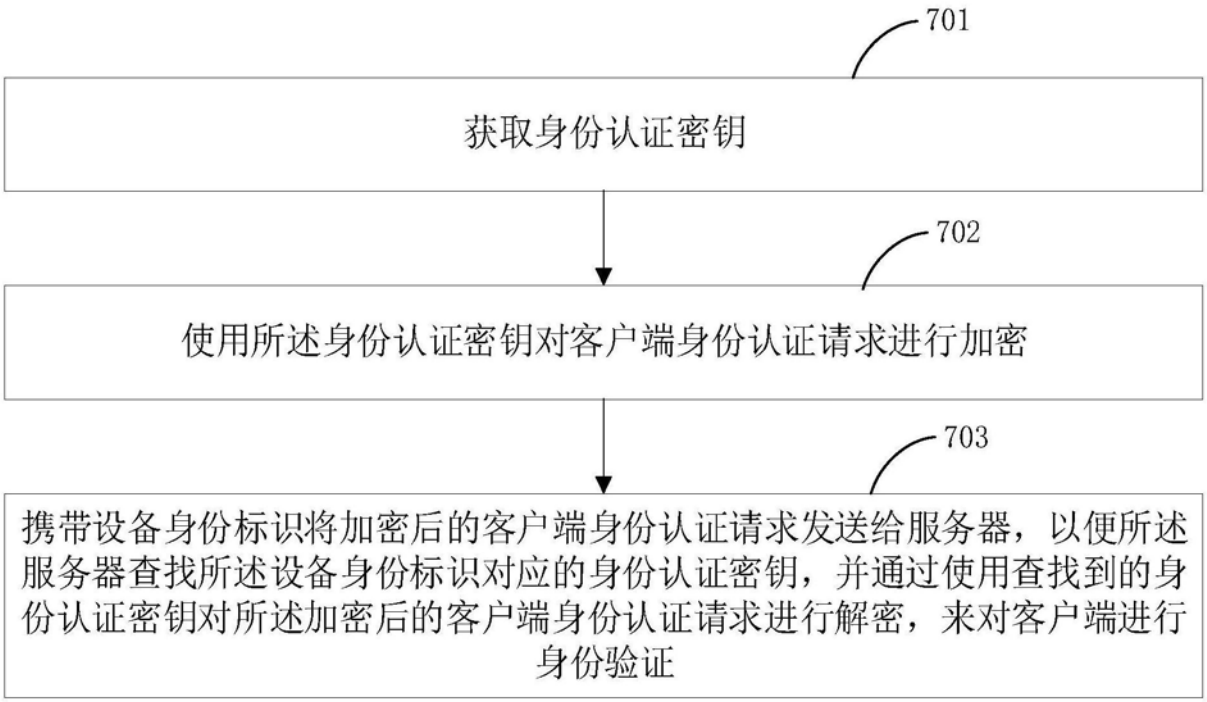

701
获取身份认证密钥
702
使用所述身份认证密钥对客户端身份认证请求进行加密
703
携带设备身份标识将加密后的客户端身份认证请求发送给服务器，以便所述服务器查找所述设备身份标识对应的身份认证密钥，并通过使用查找到的身份认证密钥对所述加密后的客户端身份认证请求进行解密，来对客户端进行身份验证

图7

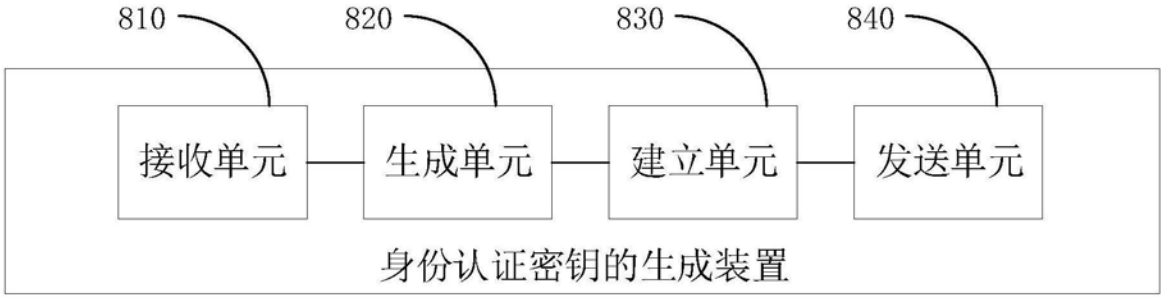

810
820
830
840
接收单元
生成单元
建立单元
发送单元
身份认证密钥的生成装置

图8

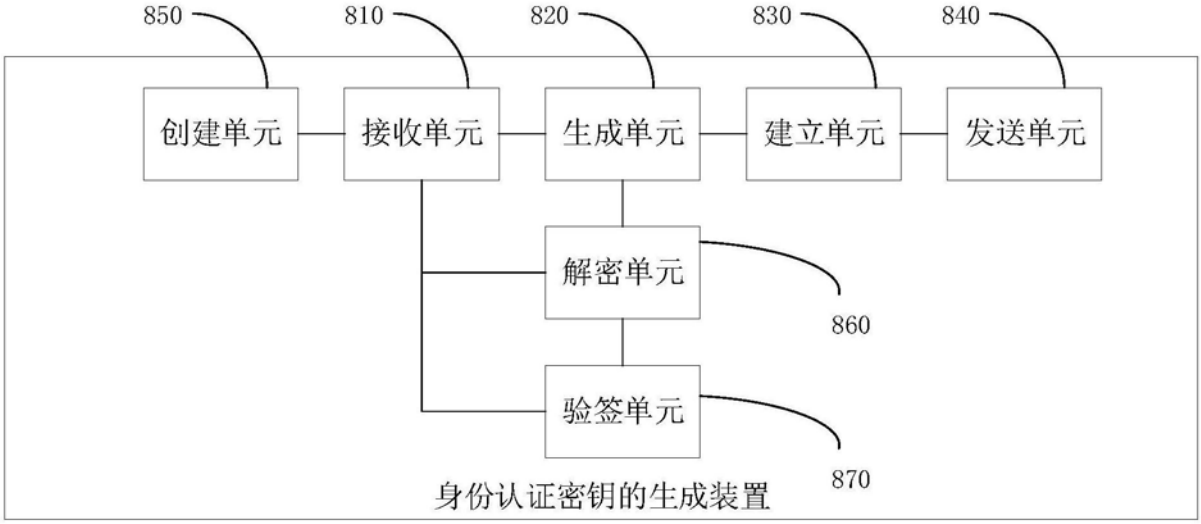

850
810
820
830
840
创建单元
接收单元
生成单元
建立单元
发送单元
解密单元
860
验签单元
870
身份认证密钥的生成装置

图9

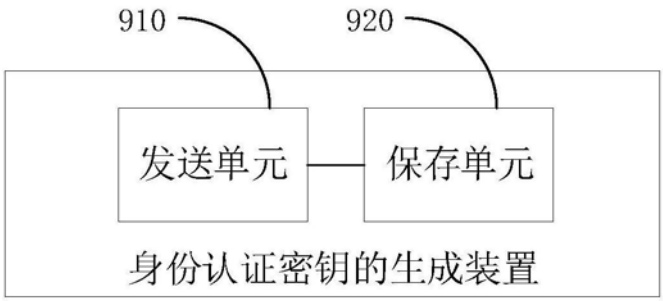

910
920
发送单元
保存单元
身份认证密钥的生成装置

图10

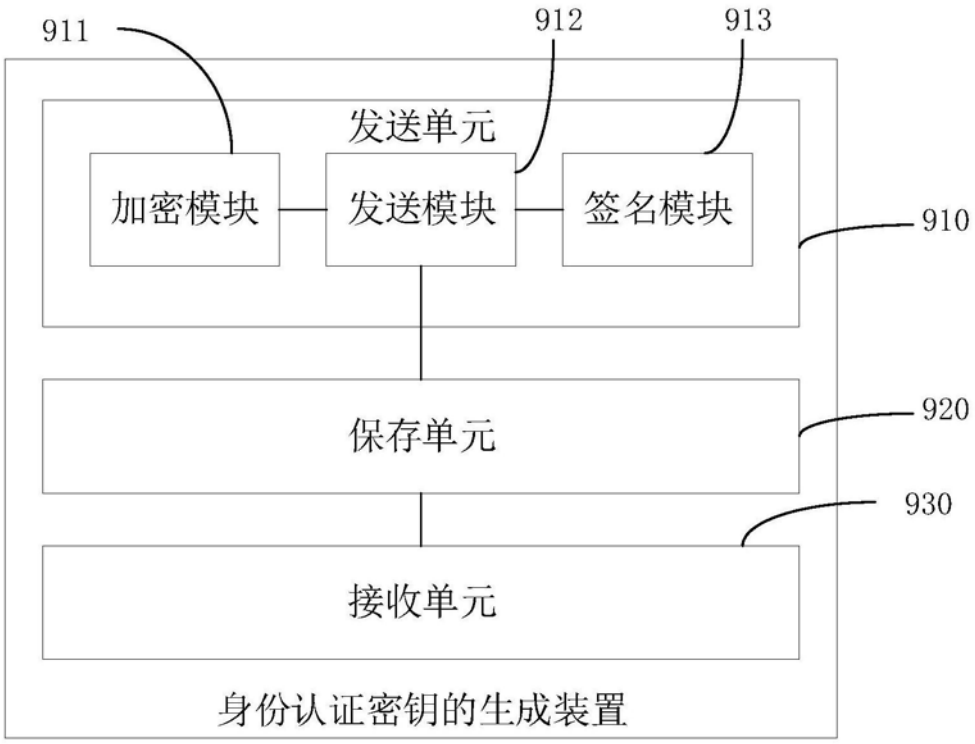

911
912
913
发送单元
加密模块
发送模块
签名模块
910
保存单元
920
930
接收单元
身份认证密钥的生成装置

图11

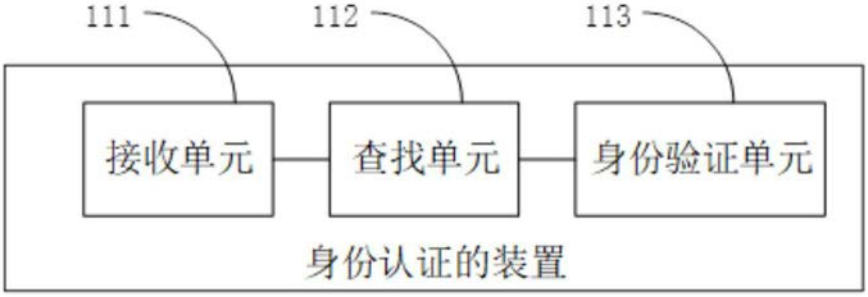

111
112
113
接收单元
查找单元
身份验证单元
身份认证的装置

图12

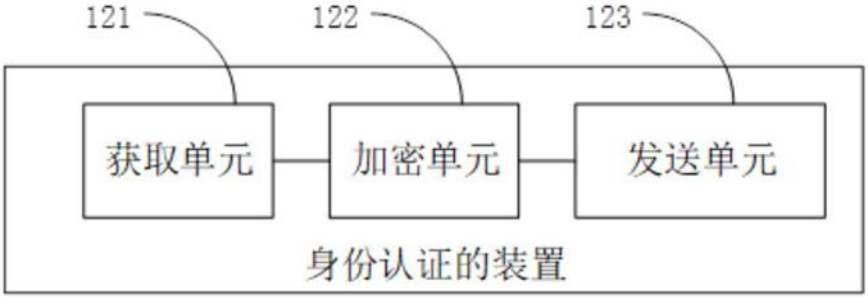

121
122
123
获取单元
加密单元
发送单元
身份认证的装置

图13