(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 115473655 A
(43)申请公布日 2022.12.13

(21)申请号 202211381768.9

(22)申请日 2022.11.07

(71)申请人 南京易科腾信息技术有限公司
地址 211100 江苏省南京市江宁区联域路3号(江宁高新园)

(72)发明人 徐锟

(74)专利代理机构 深圳紫藤知识产权代理有限公司 44570
专利代理师 远明

(51)Int.Cl.
H04L 9/32(2006.01)
H04L 9/40(2022.01)

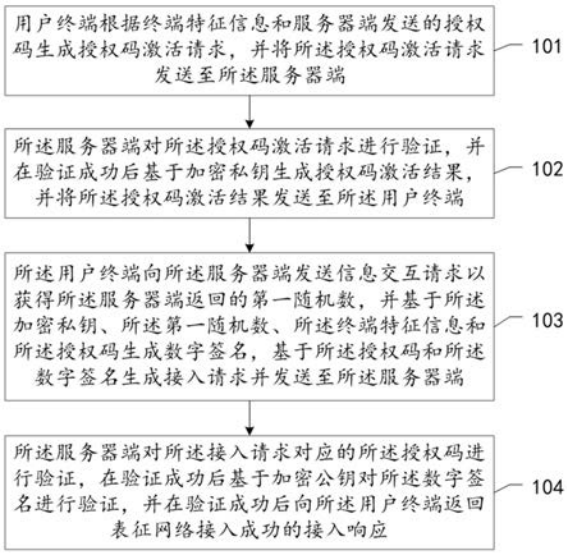
权利要求书3页 说明书11页 附图3页

(54)发明名称

接入网络的终端认证方法、装置及存储介质

(57)摘要

本发明公开了一种接入网络的终端认证方法、装置及存储介质，其中，方法包括：用户终端根据终端特征信息和服务器端发送的授权码生成授权码激活请求，并发送至服务器端；服务器端对授权码激活请求进行验证，基于加密私钥生成授权码激活结果并发送至用户终端；用户终端获得服务器端返回的第一随机数，并生成数字签名，将授权码和数字签名发送至服务器端；服务器端对授权码和数字签名进行验证，并在验证成功后向用户终端返回表征网络接入成功的接入响应。现有技术中终端设备接入网络时多采用用户名和密码的验证方式，本发明所提供的技术方案能够解决用户名和密码的验证方式存在安全风险的技术问题，提升了网络通信的安全性和可靠性。



CN 115473655 A

1.一种接入网络的终端认证方法,其特征在于,所述方法包括:

用户终端根据终端特征信息和服务器端发送的授权码生成授权码激活请求,并将所述授权码激活请求发送至所述服务器端;

所述服务器端对所述授权码激活请求进行验证,并在验证成功后基于加密私钥生成授权码激活结果,并将所述授权码激活结果发送至所述用户终端;

所述用户终端向所述服务器端发送信息交互请求以获得所述服务器端返回的第一随机数,并基于所述加密私钥、所述第一随机数、所述终端特征信息和所述授权码生成数字签名,基于所述授权码和所述数字签名生成接入请求并发送至所述服务器端;

所述服务器端对所述接入请求对应的所述授权码进行验证,在验证成功后基于加密公钥对所述数字签名进行验证,并在验证成功后向所述用户终端返回表征网络接入成功的接入响应。

2.如权利要求1所述的方法,其特征在于,所述方法还包括:

在所述用户终端根据终端特征信息和服务器端发送的授权码生成授权码激活请求之前,所述服务器端生成第二随机数,获取当前的时间戳信息,并基于所述第二随机数、所述时间戳信息和MAC地址生成所述授权码,将所述授权码储存在授权码数据集中。

3.如权利要求2所述的方法,其特征在于,所述方法还包括:

在所述基于所述第二随机数和所述时间戳信息生成所述授权码之后,所述服务器端基于公钥加密算法生成所述加密私钥和所述加密公钥,基于所述授权码、所述加密私钥和所述加密公钥为所述用户终端配置加密证书信息,并将所述授权码发送至所述用户终端。

4.如权利要求3所述的方法,其特征在于,所述方法还包括:

在所述用户终端根据终端特征信息和服务器端发送的授权码生成授权码激活请求之前,所述用户终端基于自身的至少一个设备唯一标识生成所述终端特征信息。

5.如权利要求4所述的方法,其特征在于,所述服务器端对所述授权码激活请求进行验证包括:

对所述授权码激活请求进行数据解析以得到所述授权码和所述终端特征信息,并判断所述授权码数据集中是否存在所述授权码;

若所述授权码数据集中不存在所述授权码,则确定所述授权码激活请求验证失败;

若所述授权码数据集中存在所述授权码,则判断所述终端特征信息数据集中是否存在所述授权码对应的第一实际终端特征信息;

若所述终端特征信息数据集中不存在所述第一实际终端特征信息,则将所述终端特征信息保存在所述终端特征信息数据集中,并确定所述授权码激活请求验证成功;

若所述终端特征信息数据集中存在所述第一实际终端特征信息,则判断所述第一实际终端特征信息与所述终端特征信息是否一致;

若所述第一实际终端特征信息与所述终端特征信息不一致,则确定所述授权码激活请求验证失败;

若所述第一实际终端特征信息与所述终端特征信息一致,则确定所述授权码激活请求验证成功。

6.如权利要求5所述的方法,其特征在于,所述用户终端向所述服务器端发送信息交互请求以获得所述服务器端返回的第一随机数包括:

所述用户终端基于所述授权码和/或所述终端特征信息生成请求参数，并基于所述请求参数生成所述信息交互请求，将所述信息交互请求发送至所述服务器端；

接收所述服务器端返回的与所述信息交互请求相对应的第一随机数。

7.如权利要求6所述的方法，其特征在于，所述基于所述加密私钥、所述第一随机数、所述终端特征信息和所述授权码生成数字签名包括：

所述用户终端基于所述第一随机数、所述终端特征信息和所述授权码生成第一拼接信息；

基于密码散列函数算法对所述第一拼接信息进行数据处理以得到第一哈希值；

基于所述加密私钥对所述第一哈希值进行加密以生成所述数字签名。

8.如权利要求7所述的方法，其特征在于，所述方法还包括：

在所述基于加密公钥对所述数字签名进行验证之前，所述服务器端确定与所述授权码对应的实际随机数和第二实际终端特征信息；

基于所述实际随机数、所述第二实际终端特征信息和所述授权码生成第二拼接信息。

9.如权利要求8所述的方法，其特征在于，所述基于加密公钥对所述数字签名进行验证包括：

基于所述加密公钥对所述数字签名进行解密以得到所述第一哈希值，基于密码散列函数算法对所述第二拼接信息进行数据处理以得到第二哈希值，判断所述第一哈希值和所述第二哈希值是否一致，若所述第一哈希值和所述哈希值一致，则确定所述数字签名验证成功。

10.一种接入网络的终端认证方法，用于用户终端，其特征在于，所述方法包括：

根据终端特征信息和服务器端发送的授权码生成授权码激活请求，并将所述授权码激活请求发送至所述服务器端；

接收所述服务器端返回的授权码激活结果，其中，所述服务器端对所述授权码激活请求进行验证，并在验证成功后基于加密私钥生成所述授权码激活结果；

向所述服务器端发送信息交互请求以获得所述服务器端返回的第一随机数，并基于所述加密私钥、所述第一随机数、所述终端特征信息和所述授权码生成数字签名，基于所述授权码和所述数字签名生成接入请求并发送至所述服务器端；

接收所述服务器端返回的接入响应，其中，所述服务器端对所述接入请求对应的所述授权码进行验证，在验证成功后基于加密公钥对所述数字签名进行验证，并在验证成功后向所述用户终端返回表征网络接入成功的接入响应。

11.一种接入网络的终端认证方法，用于服务器端，其特征在于，所述方法包括：

接收用户终端发送的授权码激活请求，其中，用户终端根据终端特征信息和所述服务器端发送的授权码生成所述授权码激活请求；

对所述授权码激活请求进行验证，并在验证成功后基于加密私钥生成授权码激活结果，并将所述授权码激活结果发送至所述用户终端；

接收所述用户终端发送的接入请求，其中，所述用户终端向所述服务器端发送信息交互请求以获得所述服务器端返回的第一随机数，并基于所述加密私钥、所述第一随机数、所述终端特征信息和所述授权码生成所述数字签名，基于所述授权码和所述数字签名生成接入请求；

对所述接入请求对应的所述授权码进行验证，在验证成功后基于加密公钥对所述数字签名进行验证，并在验证成功后向所述用户终端返回表征网络接入成功的接入响应。

12.一种接入网络的终端认证装置，用于用户终端，其特征在于，所述装置包括：

授权码激活请求生成模块，用于根据终端特征信息和服务器端发送的授权码生成授权码激活请求，并将所述授权码激活请求发送至所述服务器端；

授权码激活结果接收模块，用于接收所述服务器端返回的授权码激活结果，其中，所述服务器端对所述授权码激活请求进行验证，并在验证成功后基于加密私钥生成所述授权码激活结果；

数字签名发送模块，用于向所述服务器端发送信息交互请求以获得所述服务器端返回的第一随机数，并基于所述加密私钥、所述第一随机数、所述终端特征信息和所述授权码生成数字签名，基于所述授权码和所述数字签名生成接入请求并发送至所述服务器端；

接入响应接收模块，用于接收所述服务器端返回的接入响应，其中，所述服务器端对所述接入请求对应的所述授权码进行验证，在验证成功后基于加密公钥对所述数字签名进行验证，并在验证成功后向所述用户终端返回表征网络接入成功的接入响应。

13.一种接入网络的终端认证装置，用于服务器端，其特征在于，所述装置包括：

授权码激活请求接收模块，用于接收用户终端发送的授权码激活请求，其中，用户终端根据终端特征信息和所述服务器端发送的授权码生成所述授权码激活请求；

授权码激活请求验证模块，用于对所述授权码激活请求进行验证，并在验证成功后基于加密私钥生成授权码激活结果，并将所述授权码激活结果发送至所述用户终端；

接入请求接收模块，用于接收所述用户终端发送的接入请求，其中，所述用户终端向所述服务器端发送信息交互请求以获得所述服务器端返回的第一随机数，并基于所述加密私钥、所述第一随机数、所述终端特征信息和所述授权码生成所述数字签名，基于所述授权码和所述数字签名生成接入请求；

接入响应发送模块，用于对所述接入请求对应的所述授权码进行验证，对所述授权码进行验证，在验证成功后基于加密公钥对所述数字签名进行验证，并在验证成功后向所述用户终端返回表征网络接入成功的接入响应。

14.一种存储介质，其特征在于，所述存储介质中存储有多条指令，所述指令适于由处理器加载以执行如权利要求10和11中任一项所述的方法。

接入网络的终端认证方法、装置及存储介质

技术领域

[0001] 本发明涉及网络安全技术领域，尤其涉及一种接入网络的终端认证方法、装置及存储介质。

背景技术

[0002] 软件定义网络(Software Defined Network，SDN)的核心技术是将网络设备的控制面和转发面分离，从而实现网络流量的灵活控制。典型的SDN系统由一个集中的控制器软件和数量众多的转发设备组成。对比传统的网管系统，控制器软件实现了更细粒度、更灵活的网络流量调度能力。随着移动办公及驻地网运营等应用的大规模发展，控制器还需要对用户的终端接入进行控制和管理。尤其是WLAN的应用和LAN接入在电信网上大规模开展，用户终端接入数量不断增加，同时网络安全也在面临着挑战，因此有必要对终端接入进行严格的身份认证来提升网络的安全性和可靠性。

[0003] 现有技术中，对于终端接入网络的安全问题，解决方法通常是终端接入时携带用户名和密码，控制器侧对用户名和密码进行校验，实现简单，但是这种认证方式存在很多问题，尤其可能出现以下几个问题：

1)认证信息需要通过网络传递，但是很多认证系统的口令是未经加密的明文，攻击者通过窃听网络数据，则很容易提取出用户名和口令；

2)有些通信系统会将认证信息进行简单加密后进行传输，如果攻击者无法用窃听网络数据的方式推算出密码，还可能使用截取重放的方式窃取密码；

3)由于多数用户习惯使用有意义的单词或数字作为密码，一些攻击者会使用常见的数字组合或者单词来尝试窃取用户的密码；

4)攻击者利用与被攻击系统接近的机会，安装监视器或亲自窥探合法用户输入口令的过程，以得到口令；

5)攻击者冒充合法用户发送邮件或打电话给管理人员，以骗取用户口令。

[0004] 综上，当前用户名和密码的加密校验方式中，很可能遇到多种形式的网络攻击而导致数据泄露，用户名和密码的认证方式，导致用户的账户存在安全问题，用户的个人隐私无法保障。

发明内容

[0005] 本发明提供了一种接入网络的终端认证方法、装置及存储介质，旨在有效解决现有技术中用户名和密码的验证方式存在安全风险的技术问题，提升网络通信的安全性和可靠性。

[0006] 根据本发明的第一方面，本发明提供一种接入网络的终端认证方法，所述方法包括：

用户终端根据终端特征信息和服务器端发送的授权码生成授权码激活请求，并将所述授权码激活请求发送至所述服务器端；

所述服务器端对所述授权码激活请求进行验证，并在验证成功后基于加密私钥生成授权码激活结果，并将所述授权码激活结果发送至所述用户终端；

所述用户终端向所述服务器端发送信息交互请求以获得所述服务器端返回的第一随机数，并基于所述加密私钥、所述第一随机数、所述终端特征信息和所述授权码生成数字签名，基于所述授权码和所述数字签名生成接入请求并发送至所述服务器端；

所述服务器端对所述接入请求对应的所述授权码进行验证，在验证成功后基于加密公钥对所述数字签名进行验证，并在验证成功后向所述用户终端返回表征网络接入成功的接入响应。

[0007] 进一步地，所述方法还包括：

在所述用户终端根据终端特征信息和服务器端发送的授权码生成授权码激活请求之前，所述服务器端生成第二随机数，获取当前的时间戳信息，并基于所述第二随机数、所述时间戳信息和MAC地址生成所述授权码，将所述授权码储存在授权码数据集中。

[0008] 进一步地，所述方法还包括：

在所述基于所述第二随机数和所述时间戳信息生成所述授权码之后，所述服务器端基于公钥加密算法生成所述加密私钥和所述加密公钥，基于所述授权码、所述加密私钥和所述加密公钥为所述用户终端配置加密证书信息，并将所述授权码发送至所述用户终端。

[0009] 进一步地，所述方法还包括：

在所述用户终端根据终端特征信息和服务器端发送的授权码生成授权码激活请求之前，所述用户终端基于自身的至少一个设备唯一标识生成所述终端特征信息。

[0010] 进一步地，所述服务器端对所述授权码激活请求进行验证包括：

对所述授权码激活请求进行数据解析以得到所述授权码和所述终端特征信息，并判断所述授权码数据集中是否存在所述授权码；

若所述授权码数据集中不存在所述授权码，则确定所述授权码激活请求验证失败；

若所述授权码数据集中存在所述授权码，则判断所述终端特征信息数据集中是否存在所述授权码对应的第一实际终端特征信息；

若所述终端特征信息数据集中不存在所述第一实际终端特征信息，则将所述终端特征信息保存在所述终端特征信息数据集中，并确定所述授权码激活请求验证成功；

若所述终端特征信息数据集中存在所述第一实际终端特征信息，则判断所述第一实际终端特征信息与所述终端特征信息是否一致；

若所述第一实际终端特征信息与所述终端特征信息不一致，则确定所述授权码激活请求验证失败；

若所述第一实际终端特征信息与所述终端特征信息一致，则确定所述授权码激活请求验证成功。

[0011] 进一步地，所述用户终端向所述服务器端发送信息交互请求以获得所述服务器端返回的第一随机数包括：

所述用户终端基于所述授权码和/或所述终端特征信息生成请求参数，并基于所述请求参数生成所述信息交互请求，将所述信息交互请求发送至所述服务器端；

接收所述服务器端返回的与所述信息交互请求相对应的第一随机数。

[0012] 进一步地，所述基于所述加密私钥、所述第一随机数、所述终端特征信息和所述授权码生成数字签名包括：

所述用户终端基于所述第一随机数、所述终端特征信息和所述授权码生成第一拼接信息；

基于密码散列函数算法对所述第一拼接信息进行数据处理以得到第一哈希值；

基于所述加密私钥对所述第一哈希值进行加密以生成所述数字签名。

[0013] 进一步地，所述方法还包括：

在所述基于加密公钥对所述数字签名进行验证之前，所述服务器端确定与所述授权码对应的实际随机数和第二实际终端特征信息；

基于所述实际随机数、所述第二实际终端特征信息和所述授权码生成第二拼接信息。

[0014] 进一步地，所述基于加密公钥对所述数字签名进行验证包括：

基于所述加密公钥对所述数字签名进行解密以得到所述第一哈希值，基于密码散列函数算法对所述第二拼接信息进行数据处理以得到第二哈希值，判断所述第一哈希值和所述第二哈希值是否一致，若所述第一哈希值和所述哈希值一致，则确定所述数字签名验证成功。

[0015] 根据本发明的第二方面，本发明还提供了一种接入网络的终端认证方法，用于用户终端，所述方法包括：

根据终端特征信息和服务器端发送的授权码生成授权码激活请求，并将所述授权码激活请求发送至所述服务器端；

接收所述服务器端返回的授权码激活结果，其中，所述服务器端对所述授权码激活请求进行验证，并在验证成功后基于加密私钥生成所述授权码激活结果；

向所述服务器端发送信息交互请求以获得所述服务器端返回的第一随机数，并基于所述加密私钥、所述第一随机数、所述终端特征信息和所述授权码生成数字签名，基于所述授权码和所述数字签名生成接入请求并发送至所述服务器端；

接收所述服务器端返回的接入响应，其中，所述服务器端对所述接入请求对应的所述授权码进行验证，在验证成功后基于加密公钥对所述数字签名进行验证，并在验证成功后向所述用户终端返回表征网络接入成功的接入响应。

[0016] 根据本发明的第三方面，本发明还提供了一种接入网络的终端认证方法，用于服务器端，所述方法包括：

接收用户终端发送的授权码激活请求，其中，用户终端根据终端特征信息和所述服务器端发送的授权码生成所述授权码激活请求；

对所述授权码激活请求进行验证，并在验证成功后基于加密私钥生成授权码激活结果，并将所述授权码激活结果发送至所述用户终端；

接收所述用户终端发送的接入请求，其中，所述用户终端向所述服务器端发送信息交互请求以获得所述服务器端返回的第一随机数，并基于所述加密私钥、所述第一随机数、所述终端特征信息和所述授权码生成所述数字签名，基于所述授权码和所述数字签名生成接入请求；

对所述接入请求对应的所述授权码进行验证，在验证成功后基于加密公钥对所述数字签名进行验证，并在验证成功后向所述用户终端返回表征网络接入成功的接入响应。

[0017] 根据本发明的第四方面，本发明还提供了一种接入网络的终端认证装置，用于用户终端，所述装置包括：

授权码激活请求生成模块，用于根据终端特征信息和服务器端发送的授权码生成授权码激活请求，并将所述授权码激活请求发送至所述服务器端；

授权码激活结果接收模块，用于接收所述服务器端返回的授权码激活结果，其中，所述服务器端对所述授权码激活请求进行验证，并在验证成功后基于加密私钥生成所述授权码激活结果；

数字签名发送模块，用于向所述服务器端发送信息交互请求以获得所述服务器端返回的第一随机数，并基于所述加密私钥、所述第一随机数、所述终端特征信息和所述授权码生成数字签名，基于所述授权码和所述数字签名生成接入请求并发送至所述服务器端；

接入响应接收模块，用于接收所述服务器端返回的接入响应，其中，所述服务器端对所述接入请求对应的所述授权码进行验证，在验证成功后基于加密公钥对所述数字签名进行验证，并在验证成功后向所述用户终端返回表征网络接入成功的接入响应。

[0018] 根据本发明的第五方面，本发明还提供了一种接入网络的终端认证装置，用于服务器端，所述装置包括：

授权码激活请求接收模块，用于接收用户终端发送的授权码激活请求，其中，用户终端根据终端特征信息和所述服务器端发送的授权码生成所述授权码激活请求；

授权码激活请求验证模块，用于对所述授权码激活请求进行验证，并在验证成功后基于加密私钥生成授权码激活结果，并将所述授权码激活结果发送至所述用户终端；

接入请求接收模块，用于接收所述用户终端发送的接入请求，其中，所述用户终端向所述服务器端发送信息交互请求以获得所述服务器端返回的第一随机数，并基于所述加密私钥、所述第一随机数、所述终端特征信息和所述授权码生成所述数字签名，基于所述授权码和所述数字签名生成接入请求；

接入响应发送模块，用于对所述接入请求对应的所述授权码进行验证，对所述授权码进行验证，在验证成功后基于加密公钥对所述数字签名进行验证，并在验证成功后向所述用户终端返回表征网络接入成功的接入响应。

[0019] 根据本发明的第六方面，本发明还提供了一种存储介质，所述存储介质中存储有多条指令，所述指令适于由处理器加载以执行如上所述的任一接入网络的终端认证方法。

[0020] 通过本发明中的上述实施例中的一个实施例或多个实施例，至少可以实现如下技术效果：

在本发明所公开的技术方案中，通过用户终端和服务器端之间的多次身份认证，能够解决用户名和密码的验证方式存在安全风险，提升了网络通信的安全性和可靠性，能够保障用户的个人隐私。

附图说明

[0021] 下面结合附图，通过对本发明的具体实施方式详细描述，将使本发明的技术方案及其它有益效果显而易见。

[0022] 图1为本发明实施例提供的一种接入网络的终端认证方法的步骤流程图；

图2为本发明实施例提供的一种用于用户终端的接入网络的终端认证方法的步骤流程图；

图3为本发明实施例提供的一种用于服务器端的接入网络的终端认证方法的步骤流程图；

图4为本发明实施例提供的一种用于用户终端的接入网络的终端认证装置的结构示意图

图5为本发明实施例提供的一种用于服务器端的接入网络的终端认证装置的结构示意图。

具体实施方式

[0023] 下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述。显然，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域技术人员在没有作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。

[0024] 在本发明的描述中，需要说明的是，除非另有明确的规定和限定，本文中术语“和/或”，仅仅是一种描述关联对象的关联关系，表示可以存在三种关系，例如，A和/或B，可以表示：单独存在A，同时存在A和B，单独存在B这三种情况。另外，本文中字符“/”，在不做特别说明的情况下，一般表示前后关联对象是一种“或”的关系。

[0025] 图1所示为本发明实施例所提供的接入网络的终端认证方法的步骤流程图，根据本发明的第一方面，本发明提供一种接入网络的终端认证方法，所述方法包括：

步骤101：用户终端根据终端特征信息和服务器端发送的授权码生成授权码激活请求，并将所述授权码激活请求发送至所述服务器端；

步骤102：所述服务器端对所述授权码激活请求进行验证，并在验证成功后基于加密私钥生成授权码激活结果，并将所述授权码激活结果发送至所述用户终端；

步骤103：所述用户终端向所述服务器端发送信息交互请求以获得所述服务器端返回的第一随机数，并基于所述加密私钥、所述第一随机数、所述终端特征信息和所述授权码生成数字签名，基于所述授权码和所述数字签名生成接入请求并发送至所述服务器端；

步骤104：所述服务器端对所述接入请求对应的所述授权码进行验证，在验证成功后基于加密公钥对所述数字签名进行验证，并在验证成功后向所述用户终端返回表征网络接入成功的接入响应。

[0026] 本发明提出了一种基于硬件特性信息和数字签名的终端接入认证方法，以下对上述步骤101~104进行具体描述。

[0027] 在步骤101中，用户终端根据终端特征信息和服务器端发送的授权码生成授权码激活请求，并将所述授权码激活请求发送至所述服务器端；

示例性地，用户终端设备通常为个人的可通信设备，例如电脑、手机、平板或智能手表等，服务器端为控制器。当用户终端需要接入网络时，会向服务器端发送请求加入网络的信息，服务器端通过短信或者邮件的方式向用户终端返回授权码。当用户终端通过邮件、短信等方式获取到授权码后，在用户终端上携带授权码和表征硬件参数的终端特征信息向

服务器端发起授权码激活请求。

[0028] 在步骤102中，所述服务器端对所述授权码激活请求进行验证，并在验证成功后基于加密私钥生成授权码激活结果，并将所述授权码激活结果发送至所述用户终端；

示例性地，服务器端的控制器收到请求后，首先校验授权码的合法性，接着比较终端特征信息，通过该两种校验动作，可以判断用户的合法性。如果授权码激活请求通过验证，则将该授权码的私钥信息返回给用户终端设备，具体来说，服务器端确定与授权码相对应的加密私钥和加密公钥，然后基于加密私钥生成授权码激活结果，并将授权码激活结果发送至所述用户终端。用户终端设备收到授权码激活结果后，对授权码激活结果进行数据解析以得到加密私钥，并将该加密私钥保存到本地。

[0029] 步骤101和102为用户终端首次接入服务器端时的操作，目的是为了激活配置并获取加密秘钥。在用户终端将加密私钥保存在本地以后，后续需要进行网络通信而再次接入时，因为加密私钥已存在，可直接执行本方法中后续的步骤。

[0030] 此外，如果服务器端上的加密秘钥有更新的机制，则相对应地用户终端的设备也可以设置定期执行以同步最新秘钥。

[0031] 在步骤103中，所述用户终端向所述服务器端发送信息交互请求以获得所述服务器端返回的第一随机数，并基于所述加密私钥、所述第一随机数、所述终端特征信息和所述授权码生成数字签名，基于所述授权码和所述数字签名生成接入请求并发送至所述服务器端；

示例性地，当用户终端需要和服务器端进行信息交互时，用户终端首先向服务器端发送信息交互请求。服务器端在收到信息交互请求以后，基于信息交互请求生成第一随机数，并把第一随机数返回至用户终端。

[0032] 用户终端收到第一随机数后，根据第一随机数、终端特征信息和授权码生成一个拼接信息，然后在通过特定的加密算法对拼接信息进行数据处理，得到一个和拼接信息相对应的哈希值，然后再用加密私钥对哈希值进行加密以得到数字签名。在发送信息到服务器端时，同时将授权码和数字签名发送到服务器端。

[0033] 在步骤104中，所述服务器端对所述接入请求对应的所述授权码进行验证，在验证成功后基于加密公钥对所述数字签名进行验证，并在验证成功后向所述用户终端返回表征网络接入成功的接入响应。

[0034] 示例性地，服务器端收到用户终端发送的授权码和数字签名后，首先验证授权码是否合法，然后再通过加密公钥对数字签名进行解密和验证，若验证成功，则表示用户设备入网成功，服务器端向用户终端返回接入响应。

[0035] 进一步地，所述方法还包括：

在所述用户终端根据终端特征信息和服务器端发送的授权码生成授权码激活请求之前，所述服务器端生成第二随机数，获取当前的时间戳信息，并基于所述第二随机数、所述时间戳信息和MAC地址生成所述授权码，将所述授权码储存在授权码数据集中。

[0036] 进一步地，所述方法还包括：

在所述基于所述第二随机数和所述时间戳信息生成所述授权码之后，所述服务器端基于公钥加密算法生成所述加密私钥和所述加密公钥，基于所述授权码、所述加密私钥和所述加密公钥为所述用户终端配置加密证书信息，并将所述授权码发送至所述用户终

端。

[0037] 示例性地,服务器端首先会预分配一些供用户终端接入网络所需要的加密证书信息,其中,加密证书信息中包含授权码、加密公钥和加密私钥。首先可以采用UUIDv1算法来生成一个唯一识别码,具体来说,可以通过时间戳信息、第二随机数和MAC地址得到,可以保证全球唯一性。其中,通用唯一识别码(Universally Unique Identifier,UUID)方法是一种软件建构的标准,能够让分布式系统中的所有元素都能有唯一的辨识信息,不需考虑数据集创建时的名称重复问题。

[0038] 加密公钥和加密私钥可以通过公钥加密算法生成,公钥加密(Public-Key Encryption)算法是一种使用秘钥对的密码系统。通常每对秘钥包含一个公钥(Public Key)和一个私钥(Private Key)。在公钥加密系统中,一方通过公钥对明文进行加密以得到密文,另外一方通过私钥对密文进行解密得到明文,通过公钥私钥来实现数据的加密传输。

[0039] 进一步地,所述方法还包括:

在所述用户终端根据终端特征信息和服务器端发送的授权码生成授权码激活请求之前,所述用户终端基于自身的至少一个设备唯一标识生成所述终端特征信息。

[0040] 示例性地,用户终端可以从设备的数据存储中读取用于计算终端特征信息的硬件相关数据,例如设备的主板序列号、硬盘序列号等具有唯一标识的数据。

[0041] 然后根据获取到的数据计算出本设备的终端特征信息,其中,每一个用户终端的终端特征信息必须具有唯一性,不能与其它的用户终端的设备重复,且每次计算的结果相同。在具体计算时,可以根据不同的计算方法生成终端特征信息,例如可以根据主板序列号和硬盘序列号计算出一个字符串来作为终端特征信息,也可以只选择主板序列号或硬盘序列号中的一个来计算出字符串以作为终端特征信息。

[0042] 进一步地,所述服务器端对所述授权码激活请求进行验证包括:

对所述授权码激活请求进行数据解析以得到所述授权码和所述终端特征信息,并判断所述授权码数据集中是否存在所述授权码;

若所述授权码数据集中不存在所述授权码,则确定所述授权码激活请求验证失败;

若所述授权码数据集中存在所述授权码,则判断所述终端特征信息数据集中是否存在所述授权码对应的第一实际终端特征信息;

若所述终端特征信息数据集中不存在所述第一实际终端特征信息,则将所述终端特征信息保存在所述终端特征信息数据集中,并确定所述授权码激活请求验证成功;

若所述终端特征信息数据集中存在所述第一实际终端特征信息,则判断所述第一实际终端特征信息与所述终端特征信息是否一致;

若所述第一实际终端特征信息与所述终端特征信息不一致,则确定所述授权码激活请求验证失败;

若所述第一实际终端特征信息与所述终端特征信息一致,则确定所述授权码激活请求验证成功。

[0043] 示例性地,服务器端对授权码激活请求进行验证,具体来说,先对授权码激活请求进行数据解析,以获得授权码和终端特征信息。然后在授权码数据集和终端特征信息数据集分别确定是否存在授权码和终端特征信息。

[0044] 首先判断授权码数据集中是否存在授权码，如果不存在，则验证失败，并向用户终端返回激活失败结果。若授权码数据集中存在授权码，则判断是否存在授权码对应的第一实际终端特征信息，若不存在第一实际终端特征信息，则说明该授权码为初次激活，将终端特征信息写入数据存储模块中，返回激活成功。

[0045] 若存在第一实际终端特征信息，则判断第一实际终端特征信息与所述终端特征信息是不是保持一致，如果不一致，则说明该终端特征信息已被其它用户终端激活过，则向用户终端返回激活失败。

[0046] 若存在第一实际终端特征信息，且保持一致，说明之前已被同一用户终端激活过，则向用户终端返回激活成功。

[0047] 在整个认证过程中，若激活结果为失败时，则结束认证流程。如果激活结果为成功，继续认证流程，服务器端向用户终端返回的授权码激活结果中需要携带加密私钥。

[0048] 进一步地，所述用户终端向所述服务器端发送信息交互请求以获得所述服务器端返回的第一随机数包括：

所述用户终端基于所述授权码和/或所述终端特征信息生成请求参数，并基于所述请求参数生成所述信息交互请求，将所述信息交互请求发送至所述服务器端；

接收所述服务器端返回的与所述信息交互请求相对应的第一随机数。

[0049] 示例性地，用户终端的设备控制模块向服务器端的控制器认证模块发送信息交互请求时，在信息交互请求中包含请求参数，其中，请求参数包括授权码等可选信息，还可以包含用户终端的版本号或者设备的类型等信息。

[0050] 进一步地，所述基于所述加密私钥、所述第一随机数、所述终端特征信息和所述授权码生成数字签名包括：

所述用户终端基于所述第一随机数、所述终端特征信息和所述授权码生成第一拼接信息；

基于密码散列函数算法对所述第一拼接信息进行数据处理以得到第一哈希值；

基于所述加密私钥对所述第一哈希值进行加密以生成所述数字签名。

[0051] 示例性地，用户终端的设备控制模块将授权码、第一随机数以及终端特征信息进行拼接以得到第一拼接信息，然后使用SHA256算法对第一拼接结果进行计算，并得到第一哈希值，然后再用加密私钥对第一哈希值进行加密，计算出数字签名。最后将携带了授权码和数字签名的接入请求发送到服务器端。其中，SHA256是一种密码散列函数，即一个哈希函数，对于任意长度的消息，SHA256都会产生一个256bit长度的散列值，称为消息摘要，可以用一个长度为64的十六进制字符串表示。

[0052] 进一步地，所述方法还包括：

在所述基于加密公钥对所述数字签名进行验证之前，所述服务器端确定与所述授权码对应的实际随机数和第二实际终端特征信息；

基于所述实际随机数、所述第二实际终端特征信息和所述授权码生成第二拼接信息。

[0053] 进一步地，所述基于加密公钥对所述数字签名进行验证包括：

基于所述加密公钥对所述数字签名进行解密以得到所述第一哈希值，基于密码散列函数算法对所述第二拼接信息进行数据处理以得到第二哈希值，判断所述第一哈希值和

所述第二哈希值是否一致，若所述第一哈希值和所述哈希值一致，则确定所述数字签名验证成功。

[0054] 示例性地，用户终端设备向服务器端发送包含了数字签名的接入请求。服务器端到接入请求后，通过证书对用户终端设备鉴权。鉴权成功后，允许该终端设备接入与控制器进行后续交互。

[0055] 具体来说，服务器端收到接入请求后，读取数据存储中的授权码相关信息，包括该授权码已绑定的终端特征信息。服务器端校验授权码的合法性，将授权码、实际随机数、第二实际终端特征信息进行拼接后得到第二拼接信息，然后使用SHA256算法对第二拼接结果计算第二哈希值，再用加密公钥验证数字签名。如果验证通过，将接入请求结果返回给用户终端，则允许设备接入与服务器端进行后续交互。

[0056] 通过本发明中的上述实施例中的一个实施例或多个实施例，至少可以实现如下技术效果：

在本发明所公开的技术方案中，通过用户终端和服务器端之间的多次身份认证，能够解决用户名和密码的验证方式存在安全风险，提升了网络通信的安全性和可靠性，能够保障用户的个人隐私。

[0057] 基于与本发明实施例的一种接入网络的终端认证方法同样的发明构思，本发明实施例提供了一种接入网络的终端认证方法，用于用户终端，请参考图2，所述方法包括：

步骤201：根据终端特征信息和服务器端发送的授权码生成授权码激活请求，并将所述授权码激活请求发送至所述服务器端；

步骤202：接收所述服务器端返回的授权码激活结果，其中，所述服务器端对所述授权码激活请求进行验证，并在验证成功后基于加密私钥生成所述授权码激活结果；

步骤203：向所述服务器端发送信息交互请求以获得所述服务器端返回的第一随机数，并基于所述加密私钥、所述第一随机数、所述终端特征信息和所述授权码生成数字签名，基于所述授权码和所述数字签名生成接入请求并发送至所述服务器端；

步骤204：接收所述服务器端返回的接入响应，其中，所述服务器端对所述接入请求对应的所述授权码进行验证，在验证成功后基于加密公钥对所述数字签名进行验证，并在验证成功后向所述用户终端返回表征网络接入成功的接入响应。

[0058] 其中，所述用于用户终端的接入网络的终端认证方法的其它方面以及实现细节与前面所描述的接入网络的终端认证方法相同或相似，在此不再赘述。

[0059] 基于与本发明实施例的一种接入网络的终端认证方法同样的发明构思，本发明实施例提供了一种接入网络的终端认证方法，用于服务器端，请参考图3，所述方法包括：

步骤301：接收用户终端发送的授权码激活请求，其中，用户终端根据终端特征信息和所述服务器端发送的授权码生成所述授权码激活请求；

步骤302：对所述授权码激活请求进行验证，并在验证成功后基于加密私钥生成授权码激活结果，并将所述授权码激活结果发送至所述用户终端；

步骤303：接收所述用户终端发送的接入请求，其中，所述用户终端向所述服务器端发送信息交互请求以获得所述服务器端返回的第一随机数，并基于所述加密私钥、所述第一随机数、所述终端特征信息和所述授权码生成所述数字签名，基于所述授权码和所述数字签名生成接入请求；

步骤304：对所述接入请求对应的所述授权码进行验证，在验证成功后基于加密公钥对所述数字签名进行验证，并在验证成功后向所述用户终端返回表征网络接入成功的接入响应。

[0060] 其中，所述用于服务器端的接入网络的终端认证方法的其它方面以及实现细节与前面所描述的接入网络的终端认证方法相同或相似，在此不再赘述。

[0061] 基于与本发明实施例的一种接入网络的终端认证方法同样的发明构思，本发明实施例提供了一种接入网络的终端认证装置，用于用户终端，请参考图4，所述装置包括：

根据本发明的第四方面，本发明还提供了一种接入网络的终端认证装置，用于用户终端，所述装置包括：

授权码激活请求生成模块401，用于根据终端特征信息和服务器端发送的授权码生成授权码激活请求，并将所述授权码激活请求发送至所述服务器端；

授权码激活结果接收模块402，用于接收所述服务器端返回的授权码激活结果，其中，所述服务器端对所述授权码激活请求进行验证，并在验证成功后基于加密私钥生成所述授权码激活结果；

数字签名发送模块403，用于向所述服务器端发送信息交互请求以获得所述服务器端返回的第一随机数，并基于所述加密私钥、所述第一随机数、所述终端特征信息和所述授权码生成数字签名，基于所述授权码和所述数字签名生成接入请求并发送至所述服务器端；

接入响应接收模块404，用于接收所述服务器端返回的接入响应，其中，所述服务器端对所述接入请求对应的所述授权码进行验证，在验证成功后基于加密公钥对所述数字签名进行验证，并在验证成功后向所述用户终端返回表征网络接入成功的接入响应。

[0062] 其中，所述用于用户终端的接入网络的终端认证装置的其它方面以及实现细节与前面所描述的接入网络的终端认证方法相同或相似，在此不再赘述。

[0063] 基于与本发明实施例的一种接入网络的终端认证方法同样的发明构思，本发明实施例提供了一种接入网络的终端认证装置，用于服务器端，请参考图5，所述装置包括：

授权码激活请求接收模块501，用于接收用户终端发送的授权码激活请求，其中，用户终端根据终端特征信息和所述服务器端发送的授权码生成所述授权码激活请求；

授权码激活请求验证模块502，用于对所述授权码激活请求进行验证，并在验证成功后基于加密私钥生成授权码激活结果，并将所述授权码激活结果发送至所述用户终端；

接入请求接收模块503，用于接收所述用户终端发送的接入请求，其中，所述用户终端向所述服务器端发送信息交互请求以获得所述服务器端返回的第一随机数，并基于所述加密私钥、所述第一随机数、所述终端特征信息和所述授权码生成所述数字签名，基于所述授权码和所述数字签名生成接入请求；

接入响应发送模块504，用于对所述接入请求对应的所述授权码进行验证，对所述授权码进行验证，在验证成功后基于加密公钥对所述数字签名进行验证，并在验证成功后向所述用户终端返回表征网络接入成功的接入响应。

[0064] 其中，所述用于服务器端的接入网络的终端认证装置的其它方面以及实现细节与前面所描述的接入网络的终端认证方法相同或相似，在此不再赘述。

[0065] 根据本发明的第六方面，本发明还提供了一种存储介质，所述存储介质中存储有

多条指令，所述指令适于由处理器加载以执行如上所述的任一接入网络的终端认证方法。

[0066] 根据本发明的另一方面，本发明还提供一种存储介质，所述存储介质中存储有多条指令，所述指令适于由处理器加载以执行如上所述的任一接入网络的终端认证方法。

[0067] 综上所述，虽然本发明已以优选实施例揭露如上，但上述优选实施例并非用以限制本发明，本领域的普通技术人员，在不脱离本发明的精神和范围内，均可作各种更动与润饰，因此本发明的保护范围以权利要求界定的范围为准。

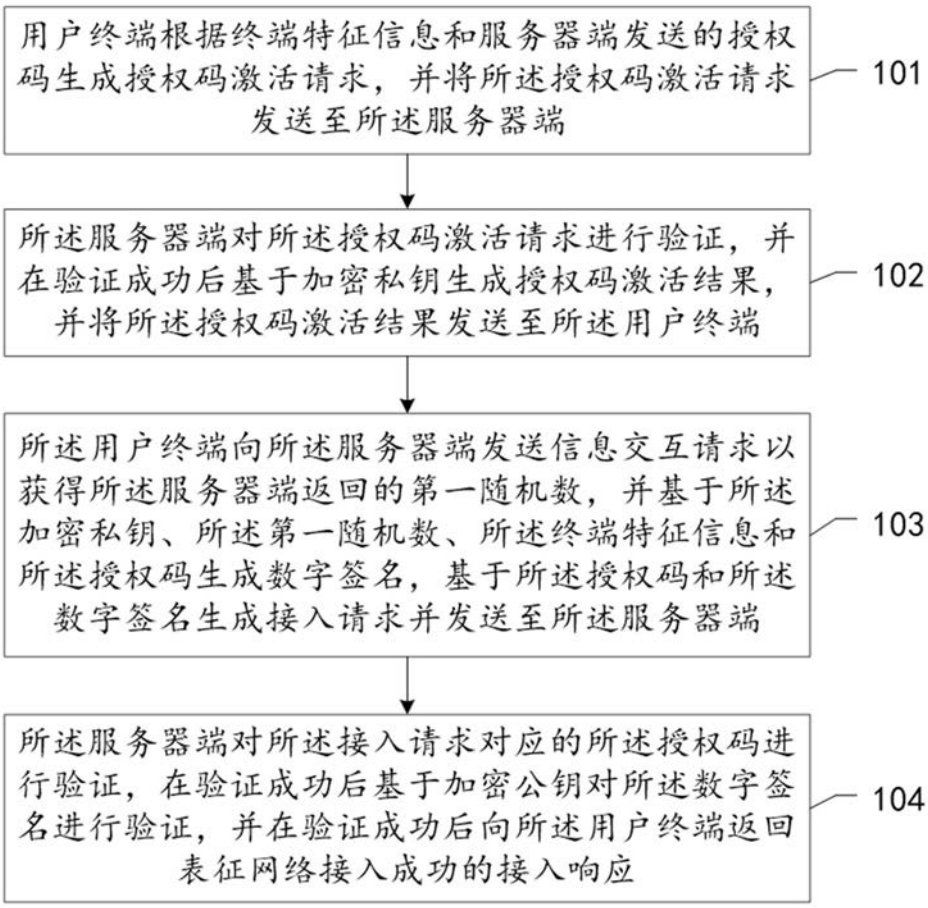

用户终端根据终端特征信息和服务器端发送的授权码生成授权码激活请求，并将所述授权码激活请求发送至所述服务器端
101
所述服务器端对所述授权码激活请求进行验证，并在验证成功后基于加密私钥生成授权码激活结果，并将所述授权码激活结果发送至所述用户终端
102
所述用户终端向所述服务器端发送信息交互请求以获得所述服务器端返回的第一随机数，并基于所述加密私钥、所述第一随机数、所述终端特征信息和所述授权码生成数字签名，基于所述授权码和所述数字签名生成接入请求并发送至所述服务器端
103
所述服务器端对所述接入请求对应的所述授权码进行验证，在验证成功后基于加密公钥对所述数字签名进行验证，并在验证成功后向所述用户终端返回表征网络接入成功的接入响应
104

图1

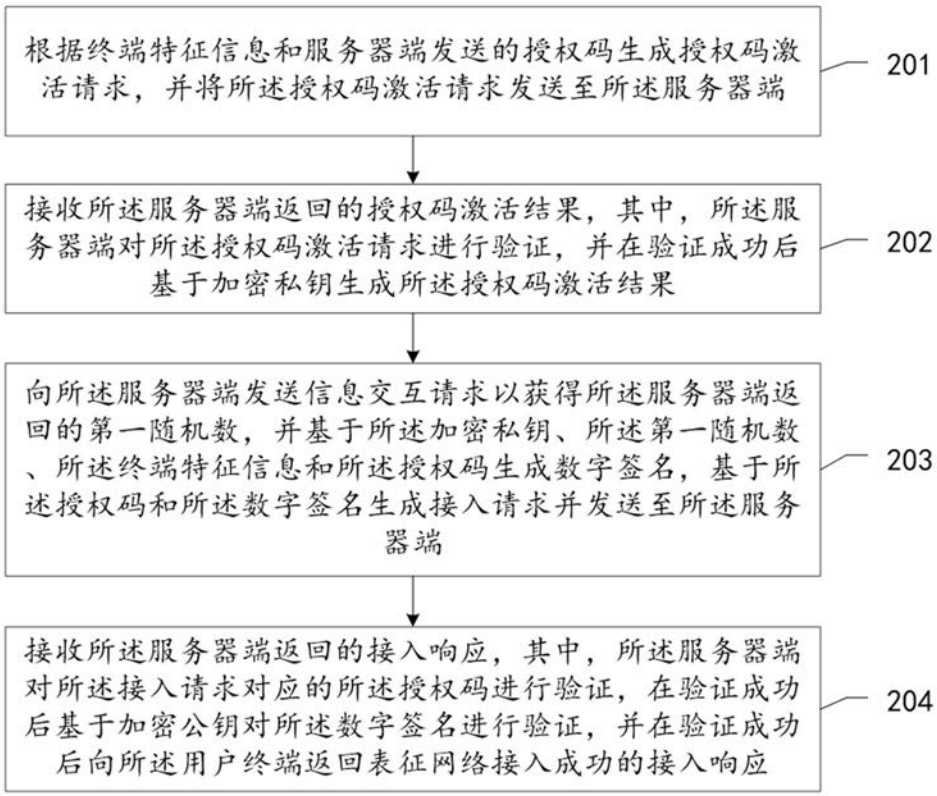

根据终端特征信息和服务器端发送的授权码生成授权码激活请求，并将所述授权码激活请求发送至所述服务器端
201
接收所述服务器端返回的授权码激活结果，其中，所述服务器端对所述授权码激活请求进行验证，并在验证成功后基于加密私钥生成所述授权码激活结果
202
向所述服务器端发送信息交互请求以获得所述服务器端返回的第一随机数，并基于所述加密私钥、所述第一随机数、所述终端特征信息和所述授权码生成数字签名，基于所述授权码和所述数字签名生成接入请求并发送至所述服务器端
203
接收所述服务器端返回的接入响应，其中，所述服务器端对所述接入请求对应的所述授权码进行验证，在验证成功后基于加密公钥对所述数字签名进行验证，并在验证成功后向所述用户终端返回表征网络接入成功的接入响应
204

图2

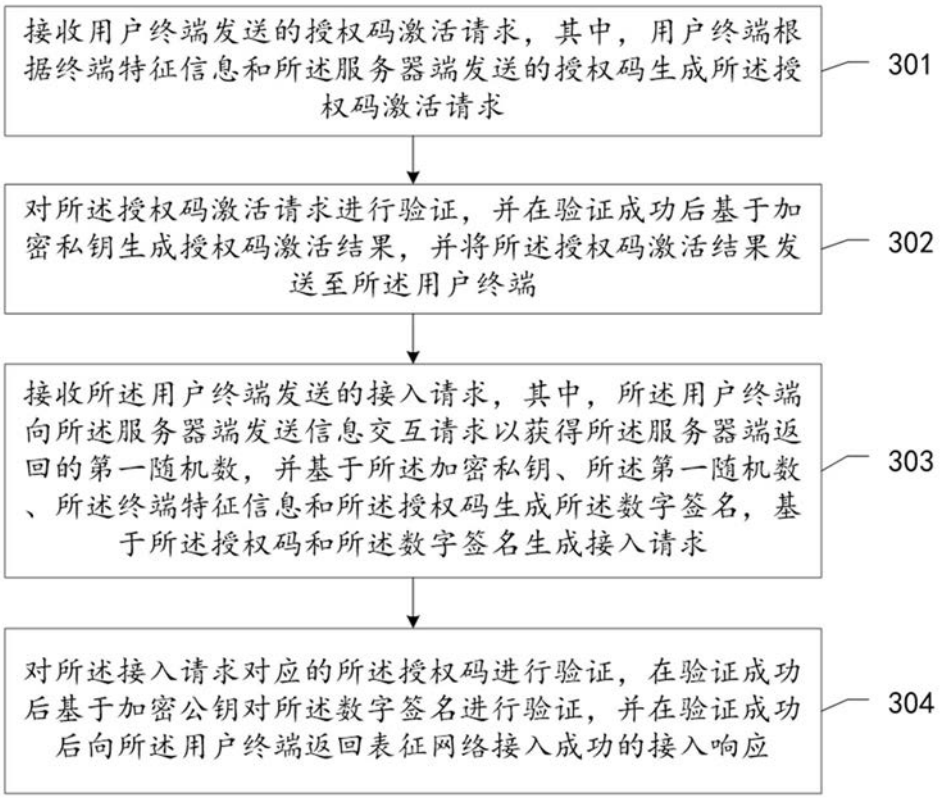

接收用户终端发送的授权码激活请求，其中，用户终端根据终端特征信息和所述服务器端发送的授权码生成所述授权码激活请求
301
对所述授权码激活请求进行验证，并在验证成功后基于加密私钥生成授权码激活结果，并将所述授权码激活结果发送至所述用户终端
302
接收所述用户终端发送的接入请求，其中，所述用户终端向所述服务器端发送信息交互请求以获得所述服务器端返回的第一随机数，并基于所述加密私钥、所述第一随机数、所述终端特征信息和所述授权码生成所述数字签名，基于所述授权码和所述数字签名生成接入请求
303
对所述接入请求对应的所述授权码进行验证，在验证成功后基于加密公钥对所述数字签名进行验证，并在验证成功后向所述用户终端返回表征网络接入成功的接入响应
304

图3


401
授权码激活请求生成模块
402
授权码激活结果接收模块
403
数字签名发送模块
404
接入响应接收模块

图4


501
授权码激活请求接收模块
502
授权码激活请求验证模块
503
接入请求接收模块
504
接入响应发送模块

图5