(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 116707983 A
(43)申请公布日 2023.09.05

(21)申请号 202310834577.1

(22)申请日 2023.07.07

(71)申请人 中国工商银行股份有限公司
地址 100140 北京市西城区复兴门内大街55号

(72)发明人 英继越 闫旭芃 邬子庄

(74)专利代理机构 中科专利商标代理有限责任公司 11021
专利代理师 樊晓

(51)Int.Cl.
H04L 9/40(2022.01)
H04L 9/08(2006.01)
H04L 9/32(2006.01)

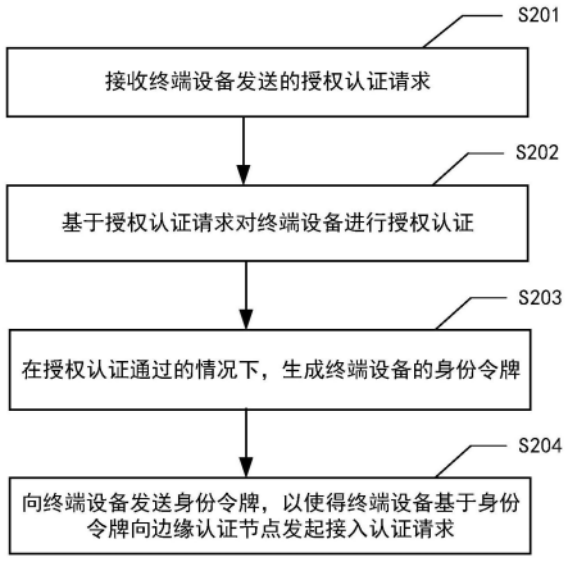
权利要求书3页 说明书21页 附图5页

(54)发明名称

授权认证方法及装置、接入认证方法及装置、设备、介质

(57)摘要

本公开提供了一种授权认证方法及装置、接入认证方法及装置、设备、介质，可以应用于信息安全技术领域、物联网技术领域、区块链技术领域、金融科技技术领域。该授权认证方法包括：接收终端设备发送的授权认证请求；基于授权认证请求对终端设备进行授权认证；在授权认证通过的情况下，生成终端设备的身份令牌；向终端设备发送身份令牌，以使得终端设备基于身份令牌向边缘认证节点发起接入认证请求。



CN 116707983 A

1.一种授权认证方法,包括:

接收终端设备发送的授权认证请求;

基于所述授权认证请求对所述终端设备进行授权认证;

在所述授权认证通过的情况下,生成所述终端设备的身份令牌;

向所述终端设备发送所述身份令牌,以使得所述终端设备基于所述身份令牌向边缘认证节点发起接入认证请求。

2.根据权利要求1所述的方法,其中,所述授权认证请求中包括授权认证信息,所述授权认证信息中包括设备公钥,所述设备公钥由所述终端设备通过执行预定密钥生成算法生成,所述预定密钥生成算法的公共参数以及所述设备公钥被发布至公共网络,由所述终端设备、所述边缘认证节点、所述授权中心共享;

基于所述授权认证请求对所述终端设备进行授权认证包括:

基于所述设备公钥对所述终端设备进行授权认证。

3.根据权利要求2所述的方法,其中,所述终端设备通过执行所述预定密钥生成算法还生成设备私钥;

基于所述设备公钥对所述终端设备进行授权认证包括:

从公共网络获取所述公共参数;

根据所述公共参数生成第一验证随机数,将所述第一验证随机数发送至所述终端设备;

接收所述终端设备发送的第二随机数签名信息,其中,所述第二随机数签名信息是由所述终端设备利用所述设备私钥对所述第一验证随机数进行签名生成的;

基于所述公共参数,利用所述设备公钥对所述第二随机数签名信息进行验证。

4.根据权利要求2所述的方法,其中,所述授权认证信息中还包括授权认证请求时间戳,在基于所述设备公钥对所述终端设备进行授权认证之前,还包括:

根据所述授权认证请求时间戳,验证所述授权认证请求的通信时长合法性。

5.根据权利要求2所述的方法,其中,生成所述终端设备的身份令牌包括:

获取令牌附加验证信息,所述令牌附加验证信息包括以下至少之一:所述终端设备的设备标识、所述身份令牌的令牌生成时间、所述身份令牌的令牌有效期;

基于所述设备公钥和所述令牌附加验证信息生成所述终端设备的身份令牌。

6.根据权利要求5所述的方法,其中,所述授权认证信息中还包括所述终端设备的设备标识以及授权认证请求时间戳,获取令牌附加验证信息包括:

基于所述授权认证请求时间戳生成令牌生成时间;

设置令牌有效期,并基于授权认证信息确定设备标识。

7.根据权利要求5所述的方法,其中,基于所述设备公钥和所述令牌附加验证信息生成所述终端设备的身份令牌包括:

通过执行所述预定密钥生成算法生成授权中心公钥和授权中心私钥,其中所述授权中心公钥被发布至公共网络,由所述终端设备、所述边缘认证节点、所述授权中心共享;

将所述设备标识、所述令牌生成时间、所述令牌有效期、所述设备公钥组装生成令牌摘要显性信息;

计算所述令牌摘要显性信息的哈希值,作为令牌摘要隐含信息;

利用所述授权中心私钥对所述令牌摘要显性信息进行签名生成令牌摘要签名信息；

将所述令牌摘要隐含信息和所述令牌摘要签名信息组装生成所述身份令牌。

8.一种接入认证方法，包括：

接收终端设备发送的接入认证请求，其中，所述接入认证请求中包括接入认证信息，所述接入认证信息中包括所述终端设备的身份令牌，所述身份令牌是由授权中心对所述终端设备进行授权认证通过的情况下生成的；

基于所述接入认证请求对所述终端设备进行接入认证。

9.根据权利要求8所述的方法，其中，基于所述接入认证请求对所述终端设备进行接入认证包括：

对所述身份令牌进行令牌认证；

在所述令牌认证通过的情况下，对所述终端设备进行密钥认证。

10.根据权利要求9所述的方法，其中：

所述身份令牌包括令牌摘要隐含信息和令牌摘要签名信息，其中，所述令牌摘要隐含信息与令牌摘要显性信息关联，所述令牌摘要显性信息包括所述终端设备的设备标识、所述身份令牌的令牌生成时间、所述身份令牌的令牌有效期、所述终端设备的设备公钥，所述令牌摘要签名信息是由授权中心利用授权中心私钥对所述令牌摘要显性信息进行签名生成的；

对所述身份令牌进行令牌认证包括：

从公共网络获取授权中心公钥；

利用所述授权中心公钥，对所述令牌摘要签名信息进行验签操作。

11.根据权利要求10所述的方法，其中，利用所述授权中心公钥，对所述令牌摘要签名信息进行验签操作包括：

利用所述授权中心公钥，对所述令牌摘要签名信息进行解密得到参考信息；

将所述参考信息的哈希值与所述令牌摘要隐含信息进行匹配；

在所述参考信息的哈希值与所述令牌摘要隐含信息相匹配的情况下，通过对所述身份令牌的令牌认证。

12.根据权利要求9所述的方法，其中，所述接入认证信息中还包括所述终端设备的设备标识；

在对所述身份令牌进行令牌认证之前，还包括：

基于所述设备标识查询受信任列表；

在所述受信任列表中不包含所述设备标识的情况下，对所述身份令牌进行令牌认证。

13.根据权利要求12所述的方法，其中，所述接入认证信息中还包括所述身份令牌的令牌生成时间、所述身份令牌的令牌有效期；

在对所述身份令牌进行令牌认证之前，还包括：

获取接入认证请求时间戳；

基于所述令牌生成时间、所述令牌有效期、所述接入认证请求时间戳，对所述身份令牌的有效期进行验证；

在所述受信任列表中不包含所述设备标识，且对所述身份令牌的有效期验证通过的情况下，对所述身份令牌进行令牌认证。

14.根据权利要求9所述的方法,其中,对所述终端设备进行密钥认证包括:

向所述终端设备发送身份挑战请求;

接收由所述终端设备发送的第二随机数签名信息,其中,所述第二随机数签名信息是由所述终端设备响应于所述身份挑战请求,基于公共参数和设备私钥对第二验证随机数进行签名生成的,所述公共参数是由所述终端设备从公共网络中获得的,所述第二验证随机数是由所述终端设备随机生成的;

从公共网络获取所述公共参数和所述终端设备的设备公钥;

基于所述公共参数,利用所述设备公钥对所述第二随机数签名信息进行验证。

15.根据权利要求8所述的方法,其中,所述接入认证信息中包括消息随机数;

在对所述终端设备进行接入认证之前,还包括:

基于所述消息随机数对所述终端设备进行防攻击验证。

16.一种授权认证装置,包括:

授权请求接收模块,用于接收终端设备发送的授权认证请求;

授权认证模块,用于基于所述授权认证请求对所述终端设备进行授权认证;

令牌生成模块,用于在所述授权认证通过的情况下,生成所述终端设备的身份令牌;

令牌发送模块,用于向所述终端设备发送所述身份令牌,以使得所述终端设备基于所述身份令牌向边缘认证节点发起接入认证请求。

17.一种接入认证装置,包括:

接入请求接收模块,用于接收终端设备发送的接入认证请求,其中,所述接入认证请求中包括接入认证信息,所述接入认证信息中包括所述终端设备的身份令牌,所述身份令牌是由授权中心对所述终端设备进行授权认证通过的情况下生成的;

接入认证模块,用于基于所述接入认证请求对所述终端设备进行接入认证。

18.一种电子设备,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,

其中,当所述一个或多个程序被所述一个或多个处理器执行时,使得所述一个或多个处理器执行根据权利要求1～15中任一项所述的方法。

19.一种计算机可读存储介质,其上存储有可执行指令,该指令被处理器执行时使处理器执行根据权利要求1～15中任一项所述的方法。

20.一种计算机程序产品,包括计算机程序,所述计算机程序被处理器执行时实现根据权利要求1～15中任一项所述的方法。

授权认证方法及装置、接入认证方法及装置、设备、介质

技术领域

[0001] 本公开涉及信息安全技术领域、物联网技术领域、区块链技术领域、金融科技技术领域，具体地涉及一种授权认证方法及装置、接入认证方法及装置、设备、介质和程序产品。

背景技术

[0002] 份认证解决的是向对方证明“我是谁”的问题，想要进行身份认证则必须具备一些物理基础比如用户持有的密码口令、密钥盘、数字证书，或者用户的特征比如指纹、虹膜、声纹、遗传信息等。

[0003] 在实现本公开构思的过程中，发明人发现相关技术中至少存在如下问题：物联网终端设备数量庞大且资源受限，传统互联网的基于数字证书的身份认证并不适用于终端设备数量庞大感知层环境，认证授权过程较为复杂，效率低下，增大了计算机处理开销以及网络传输开销。

发明内容

[0004] 鉴于上述问题，本公开提供了一种授权认证方法及装置、接入认证方法及装置、设备、介质和程序产品。

[0005] 本公开的一个方面，提供了一种授权认证方法，包括：

[0006] 接收终端设备发送的授权认证请求；

[0007] 基于授权认证请求对终端设备进行授权认证；

[0008] 在授权认证通过的情况下，生成终端设备的身份令牌；

[0009] 向终端设备发送身份令牌，以使得终端设备基于身份令牌向边缘认证节点发起接入认证请求。

[0010] 根据本公开的实施例，其中，授权认证请求中包括授权认证信息，授权认证信息中包括设备公钥，设备公钥由终端设备通过执行预定密钥生成算法生成，预定密钥生成算法的公共参数以及设备公钥被发布至公共网络，由终端设备、边缘认证节点、授权中心共享；

[0011] 基于授权认证请求对终端设备进行授权认证包括：

[0012] 基于设备公钥对终端设备进行授权认证。

[0013] 根据本公开的实施例，其中，终端设备通过执行预定密钥生成算法还生成设备私钥；

[0014] 基于设备公钥对终端设备进行授权认证包括：

[0015] 从公共网络获取公共参数；

[0016] 根据公共参数生成第一验证随机数，将第一验证随机数发送至终端设备；

[0017] 接收终端设备发送的第二随机数签名信息，其中，第二随机数签名信息是由终端设备利用设备私钥对第一验证随机数进行签名生成的；

[0018] 基于公共参数，利用设备公钥对第二随机数签名信息进行验证。

[0019] 根据本公开的实施例，其中，授权认证信息中还包括授权认证请求时间戳，在基于

设备公钥对终端设备进行授权认证之前，还包括：

[0020] 根据授权认证请求时间戳，验证授权认证请求的通信时长合法性。

[0021] 根据本公开的实施例，其中，生成终端设备的身份令牌包括：

[0022] 获取令牌附加验证信息，令牌附加验证信息包括以下至少之一：终端设备的设备标识、身份令牌的令牌生成时间、身份令牌的令牌有效期；

[0023] 基于设备公钥和令牌附加验证信息生成终端设备的身份令牌。

[0024] 根据本公开的实施例，其中，授权认证信息中还包括终端设备的设备标识以及授权认证请求时间戳，获取令牌附加验证信息包括：

[0025] 基于授权认证请求时间戳生成令牌生成时间；

[0026] 设置令牌有效期，并基于授权认证信息确定设备标识。

[0027] 根据本公开的实施例，其中，基于设备公钥和令牌附加验证信息生成终端设备的身份令牌包括：

[0028] 通过执行预定密钥生成算法生成授权中心公钥和授权中心私钥，其中授权中心公钥被发布至公共网络，由终端设备、边缘认证节点、授权中心共享；

[0029] 将设备标识、令牌生成时间、令牌有效期、设备公钥组装生成令牌摘要显性信息；

[0030] 计算令牌摘要显性信息的哈希值，作为令牌摘要隐含信息；

[0031] 利用授权中心私钥对令牌摘要显性信息进行签名生成令牌摘要签名信息；

[0032] 将令牌摘要隐含信息和令牌摘要签名信息组装生成身份令牌。

[0033] 本公开的另一个方面提供了一种接入认证方法，包括：

[0034] 接收终端设备发送的接入认证请求，其中，接入认证请求中包括接入认证信息，接入认证信息中包括终端设备的身份令牌，身份令牌是由授权中心对终端设备进行授权认证通过的情况下生成的；

[0035] 基于接入认证请求对终端设备进行接入认证。

[0036] 根据本公开的实施例，其中，基于接入认证请求对终端设备进行接入认证包括：

[0037] 对身份令牌进行令牌认证；

[0038] 在令牌认证通过的情况下，对终端设备进行密钥认证。

[0039] 根据本公开的实施例，其中：

[0040] 身份令牌包括令牌摘要隐含信息和令牌摘要签名信息，其中，令牌摘要隐含信息与令牌摘要显性信息关联，令牌摘要显性信息包括终端设备的设备标识、身份令牌的令牌生成时间、身份令牌的令牌有效期、终端设备的设备公钥，令牌摘要签名信息是由授权中心利用授权中心私钥对令牌摘要显性信息进行签名生成的；

[0041] 对身份令牌进行令牌认证包括：

[0042] 从公共网络获取授权中心公钥；

[0043] 利用授权中心公钥，对令牌摘要签名信息进行验签操作。

[0044] 根据本公开的实施例，其中，利用授权中心公钥，对令牌摘要签名信息进行验签操作包括：

[0045] 利用授权中心公钥，对令牌摘要签名信息进行解密得到参考信息；

[0046] 将参考信息的哈希值与令牌摘要隐含信息进行匹配；

[0047] 在参考信息的哈希值与令牌摘要隐含信息相匹配的情况下，通过对身份令牌的令

牌认证。

[0048] 根据本公开的实施例，其中，接入认证信息中还包括终端设备的设备标识；

[0049] 在对身份令牌进行令牌认证之前，还包括：

[0050] 基于设备标识查询受信任列表；

[0051] 在受信任列表中不包含设备标识的情况下，对身份令牌进行令牌认证。

[0052] 根据本公开的实施例，其中，接入认证信息中还包括身份令牌的令牌生成时间、身份令牌的令牌有效期；

[0053] 在对身份令牌进行令牌认证之前，还包括：

[0054] 获取接入认证请求时间戳；

[0055] 基于令牌生成时间、令牌有效期、接入认证请求时间戳，对身份令牌的有效期进行验证；

[0056] 在受信任列表中不包含设备标识，且对身份令牌的有效期验证通过的情况下，对身份令牌进行令牌认证。

[0057] 根据本公开的实施例，其中，对终端设备进行密钥认证包括：

[0058] 向终端设备发送身份挑战请求；

[0059] 接收由终端设备发送的第二随机数签名信息，其中，第二随机数签名信息是由终端设备响应于身份挑战请求，基于公共参数和设备私钥对第二验证随机数进行签名生成的，公共参数是由终端设备从公共网络中获得的，第二验证随机数是由终端设备随机生成的；

[0060] 从公共网络获取公共参数和终端设备的设备公钥；

[0061] 基于公共参数，利用设备公钥对第二随机数签名信息进行验证。

[0062] 根据本公开的实施例，其中，接入认证信息中包括消息随机数；

[0063] 在对终端设备进行接入认证之前，还包括：

[0064] 基于消息随机数对终端设备进行防攻击验证。

[0065] 本公开的另一个方面提供了一种授权认证装置，包括：

[0066] 授权请求接收模块，用于接收终端设备发送的授权认证请求；

[0067] 授权认证模块，用于基于授权认证请求对终端设备进行授权认证；

[0068] 令牌生成模块，用于在授权认证通过的情况下，生成终端设备的身份令牌；

[0069] 令牌发送模块，用于向终端设备发送身份令牌，以使得终端设备基于身份令牌向边缘认证节点发起接入认证请求。

[0070] 根据本公开的实施例，其中，授权认证请求中包括授权认证信息，授权认证信息中包括设备公钥，设备公钥由终端设备通过执行预定密钥生成算法生成，预定密钥生成算法的公共参数以及设备公钥被发布至公共网络，由终端设备、边缘认证节点、授权中心共享；

[0071] 授权认证模块包括授权认证单元，用于基于设备公钥对终端设备进行授权认证。

[0072] 根据本公开的实施例，其中，终端设备通过执行预定密钥生成算法还生成设备私钥；

[0073] 授权认证单元包括：

[0074] 获取子单元，用于从公共网络获取公共参数；

[0075] 随机数生成单元，用于根据公共参数生成第一验证随机数，将第一验证随机数发

送至终端设备；

[0076] 接收子单元，用于接收终端设备发送的第二随机数签名信息，其中，第二随机数签名信息是由终端设备利用设备私钥对第一验证随机数进行签名生成的；

[0077] 签名验证子单元，用于基于公共参数，利用设备公钥对第二随机数签名信息进行验证。

[0078] 根据本公开的实施例，其中，授权认证信息中还包括授权认证请求时间戳，上述装置还包括通信时长验证模块，用于在基于设备公钥对终端设备进行授权认证之前，根据授权认证请求时间戳，验证授权认证请求的通信时长合法性。

[0079] 根据本公开的实施例，其中，令牌生成模块包括：

[0080] 附加信息生成单元，用于获取令牌附加验证信息，令牌附加验证信息包括以下至少之一：终端设备的设备标识、身份令牌的令牌生成时间、身份令牌的令牌有效期；

[0081] 令牌生成单元，用于基于设备公钥和令牌附加验证信息生成终端设备的身份令牌。

[0082] 根据本公开的实施例，其中，授权认证信息中还包括终端设备的设备标识以及授权认证请求时间戳，附加信息生成单元包括：

[0083] 第一生成子单元，用于基于授权认证请求时间戳生成令牌生成时间；

[0084] 设置子单元，用于设置令牌有效期，并基于授权认证信息确定设备标识。

[0085] 根据本公开的实施例，其中，令牌生成单元包括：

[0086] 第二生成子单元，用于通过执行预定密钥生成算法生成授权中心公钥和授权中心私钥，其中授权中心公钥被发布至公共网络，由终端设备、边缘认证节点、授权中心共享；

[0087] 第一组装子单元，用于将设备标识、令牌生成时间、令牌有效期、设备公钥组装生成令牌摘要显性信息；

[0088] 哈希子单元，用于计算令牌摘要显性信息的哈希值，作为令牌摘要隐含信息；

[0089] 签名子单元，用于利用授权中心私钥对令牌摘要显性信息进行签名生成令牌摘要签名信息；

[0090] 第二组装子单元，用于将令牌摘要隐含信息和令牌摘要签名信息组装生成身份令牌。

[0091] 本公开的另一个方面提供了一种接入认证装置，包括：

[0092] 接入请求接收模块，用于接收终端设备发送的接入认证请求，其中，接入认证请求中包括接入认证信息，接入认证信息中包括终端设备的身份令牌，身份令牌是由授权中心对终端设备进行授权认证通过的情况下生成的；

[0093] 接入认证模块，用于基于接入认证请求对终端设备进行接入认证。

[0094] 根据本公开的实施例，其中，接入认证模块包括：

[0095] 令牌认证子模块，用于对身份令牌进行令牌认证；

[0096] 密钥认证子模块，用于在令牌认证通过的情况下，对终端设备进行密钥认证。

[0097] 根据本公开的实施例，其中：

[0098] 身份令牌包括令牌摘要隐含信息和令牌摘要签名信息，其中，令牌摘要隐含信息与令牌摘要显性信息关联，令牌摘要显性信息包括终端设备的设备标识、身份令牌的令牌生成时间、身份令牌的令牌有效期、终端设备的设备公钥，令牌摘要签名信息是由授权中心

利用授权中心私钥对令牌摘要显性信息进行签名生成的；

[0099] 令牌认证子模块包括：

[0100] 第一信息获取单元，用于从公共网络获取授权中心公钥；

[0101] 第一验签单元，用于利用授权中心公钥，对令牌摘要签名信息进行验签操作。

[0102] 根据本公开的实施例，其中，验签单元包括：

[0103] 解密子单元，用于利用授权中心公钥，对令牌摘要签名信息进行解密得到参考信息；

[0104] 匹配子单元，用于将参考信息的哈希值与令牌摘要隐含信息进行匹配；

[0105] 令牌认证子单元，用于在参考信息的哈希值与令牌摘要隐含信息相匹配的情况下，通过对身份令牌的令牌认证。

[0106] 根据本公开的实施例，其中，接入认证信息中还包括终端设备的设备标识；

[0107] 上述设备还包括查询模块，用于在对身份令牌进行令牌认证之前，基于设备标识查询受信任列表，以使得在受信任列表中不包含设备标识的情况下，对身份令牌进行令牌认证。

[0108] 根据本公开的实施例，其中，接入认证信息中还包括身份令牌的令牌生成时间、身份令牌的令牌有效期；

[0109] 上述设备还包括：

[0110] 时间戳获取模块，用于在对身份令牌进行令牌认证之前，获取接入认证请求时间戳；

[0111] 有效期验证模块，用于基于令牌生成时间、令牌有效期、接入认证请求时间戳，对身份令牌的有效期进行验证；

[0112] 处理模块，用于在受信任列表中不包含设备标识，且对身份令牌的有效期验证通过的情况下，对身份令牌进行令牌认证。

[0113] 根据本公开的实施例，其中，密钥认证子模块包括：

[0114] 挑战请求发送单元，用于向终端设备发送身份挑战请求；

[0115] 签名信息接收单元，用于接收由终端设备发送的第二随机数签名信息，其中，第二随机数签名信息是由终端设备响应于身份挑战请求，基于公共参数和设备私钥对第二验证随机数进行签名生成的，公共参数是由终端设备从公共网络中获得的，第二验证随机数是由终端设备随机生成的；

[0116] 第二信息获取单元，用于从公共网络获取公共参数和终端设备的设备公钥；

[0117] 第二验签单元，用于基于公共参数，利用设备公钥对第二随机数签名信息进行验证。

[0118] 根据本公开的实施例，其中，接入认证信息中包括消息随机数；

[0119] 上述装置还包括防攻击验证模块，用于在对终端设备进行接入认证之前，基于消息随机数对终端设备进行防攻击验证。

[0120] 本公开的另一个方面提供了一种电子设备，包括：一个或多个处理器；存储器，用于存储一个或多个程序，其中，当所述一个或多个程序被所述一个或多个处理器执行时，使得一个或多个处理器执行上述授权认证方法或接入认证方法。

[0121] 本公开的另一个方面还提供了一种计算机可读存储介质，其上存储有可执行指

令，该指令被处理器执行时使处理器执行上述授权认证方法或接入认证方法。

[0122] 本公开的另一个方面还提供了一种计算机程序产品，包括计算机程序，该计算机程序被处理器执行时实现上述授权认证方法或接入认证方法。

[0123] 根据本公开的实施例，上述授权认证方法中，授权中心对终端设备进行授权认证通过后，生成终端设备的身份令牌，该身份令牌生成后可重复使用，对于每台终端设备，仅执行一次身份认证过程为其生成身份令牌即可，身份令牌可作为终端设备的身份证明，终端设备持该身份令牌可向边缘认证节点发起多次接入认证请求。每次接入请求时仅需向边缘认证节点提供该身份令牌即可，无需边缘认证节点将终端设备的请求信息发送至认证中心进行身份认证。可见，通过上述方法实现了授权中心的轻量化，对每台设备执行一次身份认证即可，只需要在授权中心完成一次授权即可进行多次认证，以授权中心作为第三方权力中心，提供了一种一次授权、多次认证的认证方法，摒弃了传统认证中心存储管理数字证书的弊端，解决了传统方法存储、计算开销大的问题，较大程度降低认证中心的计算负担，降低了通信开销和计算量，可较好地适用于终端设备结构差异大，存储、计算资源受限的场景，具有安全、高效、轻量的优势。

附图说明

[0124] 通过以下参照附图对本公开实施例的描述，本公开的上述内容以及其他目的、特征和优点将更为清楚，在附图中：

[0125] 图1示意性示出了根据本公开实施例的授权认证方法或接入认证方法、装置、设备、介质和程序产品的应用场景图；

[0126] 图2示意性示出了根据本公开实施例的授权认证方法的流程图；

[0127] 图3示意性示出了根据本公开实施例的授权认证方法或接入认证方法的系统结构图；

[0128] 图4示意性示出了根据本公开实施例的授权认证方法的数据交互原理图；

[0129] 图5示意性示出了根据本公开实施例的接入认证方法的流程图；

[0130] 图6示意性示出了根据本公开实施例的接入认证方法的数据交互原理图；

[0131] 图7示意性示出了根据本公开实施例的授权认证装置的结构框图；

[0132] 图8示意性示出了根据本公开实施例的接入认证装置的结构框图；

[0133] 图9示意性示出了根据本公开实施例的适于实现授权认证方法或接入认证方法的电子设备的方框图。

具体实施方式

[0134] 以下，将参照附图来描述本公开的实施例。但是应该理解，这些描述只是示例性的，而并非要限制本公开的范围。在下面的详细描述中，为便于解释，阐述了许多具体的细节以提供对本公开实施例的全面理解。然而，明显地，一个或多个实施例在没有这些具体细节的情况下也可以被实施。此外，在以下说明中，省略了对公知结构和技术的描述，以避免不必要地混淆本公开的概念。

[0135] 在此使用的术语仅仅是为了描述具体实施例，而并非意在限制本公开。在此使用的术语“包括”、“包含”等表明了所述特征、步骤、操作和/或部件的存在，但是并不排除存在

或添加一个或多个其他特征、步骤、操作或部件。

[0136] 在此使用的所有术语(包括技术和科学术语)具有本领域技术人员通常所理解的含义,除非另外定义。应注意,这里使用的术语应解释为具有与本说明书的上下文相一致的含义,而不应以理想化或过于刻板的方式来解释。

[0137] 在使用类似于“A、B和C等中至少一个”这样的表述的情况下,一般来说应该按照本领域技术人员通常理解该表述的含义来予以解释(例如,“具有A、B和C中至少一个的系统”应包括但不限于单独具有A、单独具有B、单独具有C、具有A和B、具有A和C、具有B和C、和/或具有A、B、C的系统等)。

[0138] 在本公开的实施例中,所涉及的数据(例如,包括但不限于用户个人信息)的收集、更新、分析、处理、使用、传输、提供、公开、存储等方面,均符合相关法律法规的规定,被用于合法的用途,且不违背公序良俗。特别地,对用户个人信息采取了必要措施,防止对用户个人信息数据的非法访问,维护用户个人信息安全、网络安全和国家安全。

[0139] 在本公开的实施例中,在获取或采集用户个人信息之前,均获取了用户的授权或同意。

[0140] 本公开的实施例提供了一种授权认证方法,包括:

[0141] 接收终端设备发送的授权认证请求;基于授权认证请求对终端设备进行授权认证;在授权认证通过的情况下,生成终端设备的身份令牌;向终端设备发送身份令牌,以使得终端设备基于身份令牌向边缘认证节点发起接入认证请求。

[0142] 图1示意性示出了根据本公开实施例的授权认证方法或接入认证方法、装置、设备、介质和程序产品的应用场景图。

[0143] 如图1所示,根据该实施例的应用场景100可以包括终端设备101、授权中心102、边缘认证节点103。终端设备101、授权中心102、边缘认证节点103之间可通过网络进行通信。网络可以包括各种连接类型,例如有线、无线通信链路或者光纤电缆等等。

[0144] 终端设备101可以是具有显示屏并且支持网页浏览的各种电子设备,包括但不限于智能手机、平板电脑、膝上型便携计算机和台式计算机等等。

[0145] 授权中心102用于对终端设备101颁发身份令牌,可通过线下或厂商统一检测的方式对终端设备的硬件规格、版本信息、物理规格指标等信息进行检查,然后对合法设备的关键信息进行签名,生成设备的身份令牌。此过程是对终端设备接入物联网的授权。授权中心102是整个系统的核心,具备最高权力,是设备合法身份的证明者。

[0146] 边缘认证节点103可设有多个,多个边缘认证节点103可以构成的区块链网络,负责终端设备101的接入认证,例如,可在本地保存终端设备的受信任列表,与终端设备101执行基于令牌的双重认证身份认证协议,检验其身份的合法性,在接入完成后与终端设备101进行两方密钥协商,与终端设备101进行加密通信。

[0147] 根据本公开的实施例的应用场景,终端设备101在接入物联网的过程中,需要进行认证。终端设备101可从授权中心102取得身份令牌,然后向边缘认证节点103发起接入认证请求并与边缘认证节点103执行基于令牌的双重认证协议。最后与边缘认证节点103进行密钥协商,进行数据采集和加密通信。

[0148] 应该理解,图1中的终端设备101、授权中心102、边缘认证节点103的数目仅仅是示意性的。根据实现需要,可以具有任意数目的终端设备101、授权中心102、边缘认证节点

103。

[0149] 以下将基于图1描述的场景，通过图2～图9对本公开实施例的授权认证方法及接入认证方法进行详细描述。

[0150] 需要说明的是，本公开的授权认证方法及装置、接入认证方法及装置、设备、介质可以应用于信息安全技术领域、物联网技术领域、区块链技术领域、金融科技技术领域，也可用于除上述领域之外的任意领域，本公开的实施例对上述授权认证方法及装置、接入认证方法及装置、设备、介质的应用领域不做限定。

[0151] 图2示意性示出了根据本公开实施例的授权认证方法的流程图。

[0152] 如图2所示，该实施例的授权认证方法包括操作S201～操作S204。

[0153] 在操作S201，接收终端设备发送的授权认证请求；

[0154] 在操作S202，基于授权认证请求对终端设备进行授权认证；

[0155] 在操作S203，在授权认证通过的情况下，生成终端设备的身份令牌；

[0156] 在操作S204，向终端设备发送身份令牌，以使得终端设备基于身份令牌向边缘认证节点发起接入认证请求。

[0157] 图3示意性示出了根据本公开实施例的授权认证方法或接入认证方法的系统结构图。

[0158] 如图3所示，本公开实施例的授权认证方法的系统架构可以包括终端设备、授权中心(LAC)、边缘认证节点(边缘认证服务)。

[0159] 终端设备用于接入物联网进行数据交互，在接入物联网之前，需要进行认证，例如授权认证(即身份认证)和接入认证。

[0160] 终端设备、授权中心、边缘认证节点可分别通过执行预定密钥生成算法(例如基于椭圆曲线密码算法)生成各自的私钥和公钥，预定密钥生成算法的公共参数以及各自的公钥可发布至公共网络实现共享，私钥各自保存，用于在认证过程中利用私钥生成签名信息。

[0161] 在本公开实施例的应用场景下，授权中心用于对终端设备颁发身份令牌，可通过线下或厂商统一检测的方式对终端设备的硬件规格、版本信息、物理规格指标等信息进行检查，然后对合法设备的关键信息进行签名，生成设备的身份令牌。此过程是对终端设备接入物联网的授权。授权中心102是整个系统的核心，具备最高权力，是设备合法身份的证明者。

[0162] 边缘认证节点可设有多个，多个边缘认证节点可以构成区块链网络，便于通过区块链网络进行认证共识。边缘认证节点负责终端设备的接入认证，例如，可在本地保存终端设备的受信任列表，与终端设备执行基于令牌的身份认证协议，检验其身份的合法性，在接入完成后与终端设备进行两方密钥协商，与终端设备进行加密通信。

[0163] 终端设备可从授权中心取得身份令牌，然后向边缘认证节点发起接入认证请求并与边缘认证节点执行基于令牌的双重认证协议。最后与边缘认证节点进行密钥协商，进行数据采集和加密通信。

[0164] 具体地，上述操作S201～操作S204的执行主体为授权中心，主要体现授权中心对终端设备进行授权认证以颁发身份令牌的操作。

[0165] 在操作S202，授权中心对终端设备进行授权认证通过后，即通过了对终端设备的身份认证，也是对终端设备接入物联网的准入授权，授权认证通过后，生成终端设备的身份

令牌，并将身份令牌发送给终端设备，便于终端设备持该身份令牌向边缘认证节点发起接入认证请求。

[0166] 在物联网场景下，物联网终端设备数量庞大且资源受限，传统互联网的基于数字证书的身份认证通常是：终端设备向边缘服务发起接入请求，边缘服务需要在确定终端设备身份合法的情况下允许终端设备接入，但是，边缘服务自身并无法确定终端设备的身份是否合法，因此，需要将请求信息发送至认证中心，以便认证中心进行身份认证后为其返回认证结果。如此，终端设备的每次接入认证都需通过认证中心进行一次身份认证。认证授权过程较为复杂，并不适用于终端设备数量庞大感知层环境，效率低下，增大了计算机处理开销以及网络传输开销。

[0167] 根据本公开的实施例，上述授权认证方法中，授权中心对终端设备进行授权认证通过后，生成终端设备的身份令牌，该身份令牌生成后可重复使用，对于每台终端设备，仅执行一次身份认证过程为其生成身份令牌即可，身份令牌可作为终端设备的身份证明，终端设备持该身份令牌可向边缘认证节点发起多次接入认证请求。每次接入请求时仅需向边缘认证节点提供该身份令牌即可，无需边缘认证节点将终端设备的请求信息发送至认证中心进行身份认证。可见，通过上述方法实现了授权中心的轻量化，对每台设备执行一次身份认证即可，只需要在授权中心完成一次授权即可进行多次认证，可见，上述方法中，以授权中心作为第三方权力中心，提供了一种一次授权、多次认证的认证方法，摒弃了传统认证中心存储管理数字证书的弊端，解决了传统方法存储、计算开销大的问题，较大程度降低认证中心的计算负担，降低了通信开销和计算量，可较好地适用于终端设备结构差异大，存储、计算资源受限的场景，具有安全、高效、轻量的优势。

[0168] 根据本公开的实施例，具体地，授权认证请求中包括授权认证信息，授权认证信息中包括设备公钥，设备公钥由终端设备通过执行预定密钥生成算法生成，预定密钥生成算法的公共参数以及设备公钥被发布至公共网络，由终端设备、边缘认证节点、授权中心共享。

[0169] 基于此，基于授权认证请求对终端设备进行授权认证包括：基于设备公钥对终端设备进行授权认证。

[0170] 进一步地，基于设备公钥对终端设备进行身份授权认证后，可进一步基于设备公钥生成终端设备的身份令牌。

[0171] 根据本公开的实施例，设备公钥则代表设备身份，其他设备无法冒充，可基于设备公钥对终端设备进行身份授权认证。

[0172] 根据本公开的实施例，身份令牌是授权中心权威的象征，代表终端设备的合法身份，基于设备公钥生成的终端设备的身份令牌可代表设备身份。

[0173] 根据本公开的实施例，因需要基于设备公钥生成的终端设备的身份令牌，将设备公钥信息绑定至身份令牌，若公钥不合法，例如是虚假公钥，则基于设备公钥生成身份令牌则无法代表设备的合法身份，因此，需要预先对公钥的合法性进行认证，一方面，为了实现对终端设备的身份认证，另一方面也保证身份令牌的合法性。

[0174] 具体地，生成终端设备的身份令牌包括：

[0175] 首先，获取令牌附加验证信息，令牌附加验证信息包括以下至少之一：终端设备的设备标识、身份令牌的令牌生成时间、身份令牌的令牌有效期。其中，授权认证信息中还包

括终端设备的设备标识以及授权认证请求时间戳，获取令牌附加验证信息包括：基于授权认证请求时间戳生成令牌生成时间；设置令牌有效期，并基于授权认证信息确定设备标识。

[0176] 之后，基于设备公钥和令牌附加验证信息生成终端设备的身份令牌。

[0177] 根据本公开的实施例，令牌附加验证信息可用于表征设备和令牌的其他附加信息，例如，标识设备，标示令牌的生成时间和有效期之类的信息。

[0178] 根据本公开的实施例，终端设备、授权中心、边缘认证节点可分别通过执行预定密钥生成算法(例如基于椭圆曲线密码算法)生成各自的私钥和公钥，预定密钥生成算法的公共参数以及各自的公钥可发布至公共网络实现共享，私钥各自保存，用于在认证过程中利用私钥生成签名信息。

[0179] 具体地，在上述终端设备、授权中心、边缘认证节点中执行预定密钥生成算法生成私钥和公钥的方法相同，以下，以授权中心为例进行示例性说明。

[0180] 首先初始化系统，选取一个基域F_q，q是素数幂。定义在F_q上的一条椭圆曲线$E(F_q)$上的一个阶为素数n的基点P。有限域F_q、椭圆曲线参数、点P和阶数n是公共参数。

[0181] 基于预定义的公共参数，授权中心在区间[1,n-1]中随机选取一个整数d，作为授权中心私钥SK_{LAC}；

[0182] 授权中心公钥PK_{LAC}，依据算法：$Q=d\times P$计算，其中即Q为公钥PK_{LAC}。授权中心公钥被发布至公共网络，由终端设备、边缘认证节点、授权中心共享。

[0183] 按照相同的方法，终端设备从公共网络获取公共参数，执行预定密钥生成算法生成自己的设备私钥SK_{dev_i}和设备公钥PK_{dev_i}。设备公钥被发布至公共网络，由终端设备、边缘认证节点、授权中心共享。

[0184] 边缘认证节点也按照相同的方法生成自己的节点私钥和节点公钥，即生成密钥对$\{PK_{AN_i},\ SK_{AN_i}\}$。

[0185] 根据本公开的实施例，区别于传统的由一个托管中心为设备生成密钥对的方法，上述方法中，终端设备自己生成公钥私钥，私钥由设备自己保管，解决了密钥托管问题，避免密钥由托管中心保管存在的安全风险。

[0186] 图4示意性示出了根据本公开实施例的授权认证方法的数据交互原理图。

[0187] 以下结合图4对上述授权认证方法中对终端设备进行授权认证以及生成终端设备的身份令牌的方法进行具体说明。

[0188] 如图4所示，准备阶段，终端设备从公共网络获取公共参数，执行预定密钥生成算法生成自己的设备私钥SK_{dev_i}和设备公钥PK_{dev_i}。

[0189] 具体地，终端设备dev_i选取随机数$r\in[1,n-1]$，计算生成元$P_r=r\times P$，其中，为r设备私钥SK_{dev_i}，P_r为设备公钥PK_{dev_i}p,n为公共参数。

[0190] 之后，授权中心基于设备公钥对终端设备进行授权认证采用零知识证明系统中的Schnorr协议，具体包括：

[0191] 操作11、从公共网络获取公共参数；

[0192] 操作12、根据公共参数生成第一验证随机数，将第一验证随机数发送至终端设备；

[0193] 操作13、接收终端设备发送的第二随机数签名信息，其中，第二随机数签名信息是由终端设备利用设备私钥对第一验证随机数进行签名生成的；

[0194] 操作14、基于公共参数，利用设备公钥对第二随机数签名信息进行验证。

[0195] 其中，授权认证信息中还包括授权认证请求时间戳，在基于设备公钥对终端设备进行授权认证之前，还包括：根据授权认证请求时间戳，验证授权认证请求的通信时长合法性。

[0196] 参考图4，上述方法例如是：终端设备发送设备标识ID_{dev_i}、当前时间戳T_{curl}(即授权认证请求时间戳)、设备公钥P_r到授权中心，授权中心收到数据后获取当前系统时间T'_{cur}，检查请求时间$T'_{cur}-T_{curl}$是否大于认证过程单向通信时间T_{max}，该操作即为验证授权认证请求的通信时长合法性。若$T'_{cur}-T_{curl}$大于T_{max}，则则忽略当前请求，反之通信时长合法性验证通过。

[0197] 授权中心在检查时间戳合法后，根据公共参数n生成第一验证随机数，具体地，生成第一验证随机数$c\in[1,n-1]$，发送到终端设备。

[0198] 终端设备利用设备私钥对第一验证随机数进行签名生成第二随机数签名信息。计算得到第二随机数签名信息z，可以将该签名信息与时间戳一起发送到授权中心。

[0199] 第二随机数签名信息的计算方法参考下式(1)：

[0200] $$z = r + c \times SK_{dev_i} \quad \text{----} \quad (1)$$

[0201] 授权中心接收终端设备发送的第二随机数签名信息后，基于公共参数p，利用设备公钥PK_{dev_i}对第二随机数签名信息进行验证，具体地验证下式(2)是否成立：

[0202] $$z \times P = P_r + c \times PK_{dev_i} \text{----} \quad (2)$$

[0203] 若成立，则验证通过，证明设备密钥合法，说明SK_{dev_i}为PK_{dev_i}对应的私钥，完成了在零知识情况下的密钥验证，设备的身份认证通过。

[0204] 根据本公开的实施例，通过零知识证明协议，降低在认证过程中私钥暴露的风险，且通过零知识证明提升协议安全性，在本协议中简化的报文结构降低复杂度，该认证协议算法在加密算法的选择和密文的长度上具备一定优势，可降低加解密过程的计算开销和数据传输的通信开销，更适用于资源受限的物联网环境。

[0205] 根据本公开的实施例，如图4所示，对设备密钥认证通过后，授权中心使用签名算法生成设备dev_i的令牌。

[0206] 令牌附加验证信息包括终端设备的设备标识、身份令牌的令牌生成时间、身份令牌的令牌有效期。基于设备公钥和令牌附加验证信息生成终端设备的身份令牌包括：

[0207] 操作21、通过执行预定密钥生成算法生成授权中心公钥和授权中心私钥，其中授权中心公钥被发布至公共网络，由终端设备、边缘认证节点、授权中心共享；

[0208] 操作22、将设备标识、令牌生成时间、令牌有效期、设备公钥组装生成令牌摘要显性信息M；如下式(3)

[0209] $$M = \{PK_{dev_i} \| ID_{dev_i} \| T_{dev_i} \| T_{val}\} \quad \text{----} \quad (3)$$

[0210] 其中T_{dev_i}为令牌生成时间，T_{val}为设备的有效期。

[0211] 令牌生成时间可根据当前时间戳T_{curl}，即授权请求时间戳确定。

[0212] 操作23、计算令牌摘要显性信息M的哈希值，作为令牌摘要隐含信息：$H_{dev_i} = H(M)$。

[0213] 操作24、利用授权中心私钥SK_{LAc}对令牌摘要显性信息M进行签名生成令牌摘要签名信息:$Sign(M,SK_{LAC})$;

[0214] 操作25、将令牌摘要隐含信息和令牌摘要签名信息组装生成身份令牌$token_{dev_i}$。如下式(4):

[0215] $$token_{dev_i} = \{H_{dev_i} \| Sign(M, SK_{LAC})\} \quad ---- \quad (4)。$$

[0216] 根据本公开的实施例,授权中心代替传统的认证中心CA的功能,身份令牌代替数字证书,在终端设备授权取得令牌的阶段,采用了具有零知识性质的Schnorr协议进行终端公钥的绑定,生成了设备的身份令牌。

[0217] 本公开的另一个方面提供了一种接入认证方法,图5示意性示出了根据本公开实施例的接入认证方法的流程图。

[0218] 如图5所示,该实施例的接入认证方法包括操作S501～操作S502。

[0219] 在操作S501,接收终端设备发送的接入认证请求,其中,接入认证请求中包括接入认证信息,接入认证信息中包括终端设备的身份令牌,身份令牌是由授权中心对终端设备进行授权认证通过的情况下生成的;

[0220] 在操作S502,基于接入认证请求对终端设备进行接入认证。

[0221] 具体地,上述操作S501～操作S502的执行主体为边缘认证节点,主要体现边缘认证节点对终端设备进行接入认证的操作。

[0222] 根据本公开的实施例,接入认证信息中包括终端设备的身份令牌,因该身份令牌是授权中心对终端设备进行授权认证通过后生成的,该身份令牌生成后可重复使用,对于每台终端设备,仅执行一次身份认证过程为其生成身份令牌即可,身份令牌可作为终端设备的身份证明,终端设备持该身份令牌可向边缘认证节点发起多次接入认证请求。终端设备每次接入请求时仅需向边缘认证节点提供该身份令牌即可,无需边缘认证节点将终端设备的请求信息发送至认证中心进行身份认证。通过上述方法实现了授权中心的轻量化,对每台设备执行一次身份认证即可,只需要在授权中心完成一次授权即可进行多次认证,摒弃了传统认证中心存储管理数字证书的弊端,解决了传统方法存储、计算开销大的问题,较大程度降低认证中心的计算负担,降低了通信开销和计算量,可较好地适用于终端设备结构差异大,存储、计算资源受限的场景,具有安全、高效、轻量的优势。

[0223] 具体地,边缘认证节点对终端设备进行接入认证包括双重认证:令牌认证+密钥认证。例如,基于接入认证请求对终端设备进行接入认证包括:

[0224] 首先,对身份令牌进行令牌认证。

[0225] 之后,在令牌认证通过的情况下,对终端设备进行密钥认证。

[0226] 图6示意性示出了根据本公开实施例的接入认证方法的数据交互原理图。以下结合图6对本公开实施例的接入认证方法进行详细说明。

[0227] 如图6所示,接入请求的接入认证信息中可包括终端设备的身份令牌$token_{dev_i}$、终端设备的设备标识ID_{dev_i}、身份令牌的令牌生成时间T_{dev_i}、身份令牌的令牌有效期T_{val}、设备公钥PK_{dev_i}、消息随机数R_{msg}等信息。终端设备将这些信息发送至距离该设备通信开销最小的边缘认证节点。

[0228] 边缘认证节点在对终端设备进行令牌认证之前,可以先基于消息随机数对终端设

备进行防攻击验证。若不合法则拒绝接入，返回消息错误信息。例如，同一时间段内该终端设备发送的多条请求的消息随机数相同，则认为该设备有攻击边缘认证节点的风险拒绝接入。

[0229] 边缘认证节点同时可根据请求时间戳检查通信时长的合法性，若不合法则拒绝接入，返回消息错误信息。

[0230] 如图6所示，根据本公开的实施例，在对身份令牌进行令牌认证之前，还可以包括：

[0231] 基于设备标识查询受信任列表；若受信任列表中包含该设备标识，则说明此前该设备的身份令牌已经经过认证，则不对其进行令牌认证，直接进行第二步的密钥认证。在受信任列表中不包含设备标识的情况下，对身份令牌进行令牌认证。

[0232] 根据本公开的实施例，在对身份令牌进行令牌认证之前，还包括验证令牌的有效期。若该令牌已过期，则无需进行令牌认证，拒绝接入，返回消息错误信息，并在受信任列表中删除此信息，仅对在有效期内的令牌进行认证。

[0233] 验证令牌的有效期具体包括：

[0234] 操作31、获取接入认证请求时间戳T_{cur2}；

[0235] 操作32、基于令牌生成时间T_{dev_i}、令牌有效期T_{val}、接入认证请求时间戳T_{cur2}，对身份令牌的有效期进行验证；

[0236] 具体地，若$T_{dev_i} + T_{val} < T_{cur2}$，则说明令牌已失效，拒绝接入。反之，验证通过。

[0237] 操作33、在受信任列表中不包含设备标识，且对身份令牌的有效期验证通过的情况下，对身份令牌进行令牌认证。

[0238] 根据本公开的实施例，对身份令牌进行令牌认证包括：

[0239] 从公共网络获取授权中心公钥；利用授权中心公钥，对令牌摘要签名信息进行验签操作。

[0240] 参考上述实施例，身份令牌包括令牌摘要隐含信息和令牌摘要签名信息，其中，令牌摘要隐含信息与令牌摘要显性信息关联，令牌摘要显性信息包括终端设备的设备标识、身份令牌的令牌生成时间、身份令牌的令牌有效期、终端设备的设备公钥，令牌摘要签名信息是由授权中心利用授权中心私钥对令牌摘要显性信息进行签名生成的。

[0241] 具体地，利用授权中心公钥，对令牌摘要签名信息进行验签操作包括：

[0242] 操作41、利用授权中心公钥，对令牌摘要签名信息进行解密得到参考信息；因令牌摘要签名信息$Sign(M,SK_{LAC})$是由授权中心利用授权中心私钥SK_{LAC}对令牌摘要显性信息M进行签名生成的，因此，可利用授权中心公钥PK_{LAC}，对令牌摘要签名信息进行解密得到参考信息$Verify(Sign(M,SK_{LAC}),PK_{LAC})$。若密钥合法，则$Verify(Sign(m,SK_{LAC}),PK_{LAC})=M$。

[0243] 操作42、将参考信息的哈希值与令牌摘要隐含信息进行匹配；

[0244] 操作43、在参考信息的哈希值与令牌摘要隐含信息相匹配的情况下，通过对身份令牌的令牌认证。

[0245] 即验证$H(Verify(Sign(M,SK_{LAC}),PK_{LAC}))$与$H_{dev_i}$，即与H(M)是否相等。若密钥合法，则$H(Verify(Sign(M,SK_{LAC}),\ PK_{LAC}))=H_{dev_i}=H(M)$，通过对身份令牌的令牌认证。

[0246] 根据本公开的实施例，因授权中心在授权阶段给予授权中心私钥生成了令牌的签

名信息，因此，边缘认证节点可利用授权中心公钥，对令牌摘要签名信息进行验签，已验证身份令牌的合法性。通过该方法，一方面可提高令牌信息安全性，另一方面认证过程算法所需参数较少，节约了通信开销，提高了认证效率。

[0247] 通过使用认证服务器的对终端设备的公钥和有效时间戳进行签名生成设备身份令牌的方式代替了数字证书，一方面设备的私钥由设备自己生成，认证服务器无法感知，解决了密钥托管的问题。另一方面令牌证明了设备身份的合法性，通过验证令牌的方式可以防止非法设备接入。最关键的一点是令牌认证的方式解决了第三方可信中心数字证书的存储和管理问题，减轻了终端设备的计算压力，降低了通信开销。

[0248] 根据本公开的实施例，在通过对终端设备的身份令牌的认证后，对终端设备进行密钥认证包括：

[0249] 操作51、向终端设备发送身份挑战请求；

[0250] 操作52、接收由终端设备发送的第二随机数签名信息，其中，第二随机数签名信息是由终端设备响应于身份挑战请求，基于公共参数和设备私钥对第二验证随机数进行签名生成的，公共参数是由终端设备从公共网络中获得的，第二验证随机数是由终端设备随机生成的；

[0251] 操作53、从公共网络获取公共参数和终端设备的设备公钥；

[0252] 操作54、基于公共参数，利用设备公钥对第二随机数签名信息进行验证。

[0253] 如图6所示，边缘认证节点在检查设备的令牌合法性结束后，需要对设备的公钥和私钥进行认证。

[0254] 首先由边缘认证节点向终端设备发送身份挑战请求，终端设备收到挑战后进行如下操作：

[0255] 基于公共参数，选取一个随机数k∈[1,n-1]，按照下式(5)、(6)计算点：

[0256] $k\times P=(x_1,y_1)$ ----(5)

[0257] $R=x_1 \bmod n$----(6)

[0258] 若R＝0，则重新选取随机数进行计算。

[0259] 按照下式(7)计算：

[0260] $k^{-1} \bmod n$----(7)

[0261] 选取第二验证随机数m，计算哈希值z＝H(m)

[0262] 检查$S = k^{-1}(z + SK_{dev_i} \times P) \bmod n$是否为0，若为0则重新选取随机数k。直至确定合适的参数k。

[0263] 终端设备基于公共参数和设备私钥对第二验证随机数m进行签名生成第二随机数签名信息(R,S)。

[0264] 之后，终端设备将第二随机数签名信息发送边缘认证节点。同时可发送消息时间戳T_{cur3}，消息随机数R_{msg}。例如，终端设备将{m,R,S,R_{msg},T_{cur}}等信息传送给边缘认证节点。

[0265] 边缘认证节点收到终端发来的挑战信息后，首先检查消息随机数和消息时间戳的合法性，若合法则进行挑战信息检验，否则拒绝接入。

[0266] 边缘认证节点进行挑战信息检验为：基于公共参数，利用设备公钥对第二随机数签名信息进行验证。

[0267] 进行验证的具体算法可参考下式(8)～(13)。

[0268] 计算参数：

[0269] $e' = H(m)$ ----(8)

[0270] $w = S^{-1} \bmod n$ ----(9)

[0271] $u_1 = e' \times w \bmod n$ ----(10)

[0272] $u_2 = R \times w \bmod n$ ----(11)

[0273] 计算点：

[0274] $$X = u_1 \times P + u_2 \times PK_{dev_i} = (x_2, y_2) \text{----} \quad (12)$$

[0275] 若$x_2 = 0$，则说明验证失败，拒绝接入，否则计算参数

[0276] $v = x_2 \bmod n$ ----(13)

[0277] 若$v = r$，则说明验证成功。

[0278] 如图6所示，根据本公开的实施例，进一步地，边缘认证节点可设有多个，多个边缘认证节点可以构成区块链网络，便于通过区块链网络进行认证共识。

[0279] 在当前节点通过对待终端设备的接入认证后，可进一步将认证信息发布到区块链中，通过所有节点对认证信息的共识来决定对终端设备的接入。如此，可进一步加强认证的安全性和可靠性。

[0280] 例如，若当前节点是被不安全的节点，则即便该节点对设备接入认证通过，也无法保证认证的可靠性，通过将认证信息发布到区块链中，所有节点对该终端设备的接入认证都通过的情况下，通过对该终端设备的最终接入认证。

[0281] 认证信息例如包括：ID_{dev_i}，PK_{dev_i}，$token_{dev_i}$，m，R，S。

[0282] 当终端设备的认证共识通过后，将设备信息添加到受信任列表中，同时此设备的接入认证申请被通过。

[0283] 根据本公开的实施例，为了进一步说明本公开实施例的认证方法的可靠性，以下设想几种攻击方式，以说明本公开实施例中认证算法的可靠性。

[0284] 例如，某用户想要冒充或伪造身份，需要获得设备或节点的私钥。如果设备在认证过程中签名所使用的随机数k被攻击者获得，那么攻击者可以根据随机数k计算点R：

[0285] $P_R = k \times P = (x_R, y_R)$

[0286] 然后通过

[0287] $R = x_R \bmod n$

[0288] 再窃取到设备的签名信息{m，R，S}，通过计算

[0289] $P_r = R^{-1}(S \times k - H(m)) \bmod n$

[0290] 得到用户的私钥P_r，由于终端设备的公钥和令牌对外公开，则攻击者就可以通过持有用户私钥的方式冒充终端身份，伪造签名。

[0291] 具体地，例如采用随机碰撞法进行破解随机数k。

[0292] 用户通过随机生成的k^1，计算$P_R^1 = k^1 \times P = (x_R^1, y_R^1)$，然后计算$R^1 = x_R^1 \bmod n$，最后查找通信过程中的签名信息{m，R，S}，看是否存在$R^1 = R$，若存在，则可以计算出该节点的私钥。

[0293] 由于本公开实施例采用的随机数生成算法使随机数k在值空间内的分布概率均

匀，若k的比特长度为n，则每次试探k的成功率是$\frac{1}{2^n}$，本文采用的比特长度为256，则成功概率为$\frac{1}{2^{256}}$，因此通过随机碰撞进行攻击几乎是不可能的。

[0294] 再例如，假设存在u个问题终端设备，这里的问题终端设备是指意图获取其他设备私钥进行身份冒充的设备。每个终端设备dev_i在每次生成自己的签名时会在本地存储下自己生成签名时使用的随机数$\{k_{i_1}, k_{i_2}, k_{i_3}, \cdots\}$和对应的$\{R_{i_1}, R_{i_2}, R_{i_3}, \cdots\}$，然后不断的获取网络中签名信息，检查是否存在签名$R \in \{R_{i_1}, R_{i_2}, R_{i_3}, \cdots\}$，如果存在进行上述计算得到对应的私钥。

[0295] 在最坏情况下，网络中的所有节点都是问题节点，即参与认证的各方都会保存用于生成签名的随机数和签名，在这种情况下，发生私钥被计算出来的概率问题转化为：在整个通信网络中的所有签名信息中至少存在两个签名使用了同一个随机数k。那么在k分布均匀的情况下(长度为n比特)，根据生日攻击理论，当网络中签名的的数量为N时，敌手会有

[0296] 1-p的概率攻击成功，其中$p = e^{-\frac{N(N-1)}{2^{n+1}}}$。代入n＝256时，假设敌手以0.01以上的概率攻击成功，则需要$N \geq 2^{126}$，假设敌手以1×10^{-10}的概率攻击成功则也要求$N \geq 2^{113}$。终端设备每隔10分钟认证一次，一共10000个设备，认证100年产生的签名数为$24 \times 6 \times 10000 \times 365 \times 100 \approx 2^{36}$远远达不到$2^{113}$。

[0297] 以下，对本公开实施例设计的认证协议的安全性进行非形式化分析：

[0298] 抗伪造攻击：当攻击者使用伪造合法设备的认证请求进行访问时，访问会被拒绝，因为伪造者并不持有合法设备的私钥，因此无法完成认证挑战，区块链网络会拒绝接入。

[0299] 抗重放攻击：不同设备之间和节点之间的通信数据包会携带唯一的时间戳和随机数，在通信过程中若攻击者使用重复的数据包进行重放攻击，认证节点会验证随机数和时间戳，将其抛弃。

[0300] 由于每次认证请求的通信数据包都有设备和认证节点的私钥签名，并且写入到区块链中，所以终端设备无法否认自己的认证请求。

[0301] 可溯源：每个终端成功通过接入认证之后，它的认证信息都会加上时间戳打包写入区块链中，区块链中的信息都通过哈希函数生成了完整性摘要，并通过Merkle树保证了信息的无法篡改，确保了溯源信息的真实性。

[0302] 在本协议中，第三方权威机构是授权中心LAC，在授权过程中使用具有零知识性质的Schnorr协议进行终端设备的私钥认证，在协议交互过程中不会透露任何有关终端设备私钥的信息。相比于传统公钥验签的认证方式，虽然多了交互过程，但是在一定程度上保证了设备私钥的安全性，降低了私钥泄漏的风险。

[0303] 基于上述授权认证方法，本公开还提供了一种授权认证装置。以下将结合图7对该装置进行详细描述。

[0304] 图7示意性示出了根据本公开实施例的授权认证装置的结构框图。

[0305] 如图7所示，该实施例的授权认证装置700包括授权请求接收模块701、授权认证模块702、令牌生成模块703、令牌发送模块704.

[0306] 授权请求接收模块701，用于接收终端设备发送的授权认证请求；

[0307] 授权认证模块702，用于基于授权认证请求对终端设备进行授权认证；

[0308] 令牌生成模块703，用于在授权认证通过的情况下，生成终端设备的身份令牌；

[0309] 令牌发送模块704，用于向终端设备发送身份令牌，以使得终端设备基于身份令牌向边缘认证节点发起接入认证请求。

[0310] 根据本公开的实施例，通过授权认证模块702对终端设备进行授权认证通过后，通过令牌生成模块703生成终端设备的身份令牌，该身份令牌生成后可重复使用，对于每台终端设备，仅执行一次身份认证过程为其生成身份令牌即可，身份令牌可作为终端设备的身份证明，终端设备持该身份令牌可向边缘认证节点发起多次接入认证请求。每次接入请求时仅需向边缘认证节点提供该身份令牌即可，无需边缘认证节点将终端设备的请求信息发送至认证中心进行身份认证。可见，通过上述装置实现了授权中心的轻量化，对每台设备执行一次身份认证即可，只需要在授权中心完成一次授权即可进行多次认证，提供了一种一次授权、多次认证的认证方法，摒弃了传统认证中心存储管理数字证书的弊端，解决了传统方法存储、计算开销大的问题，较大程度降低认证中心的计算负担，降低了通信开销和计算量，可较好地适用于终端设备结构差异大，存储、计算资源受限的场景，具有安全、高效、轻量的优势。

[0311] 根据本公开的实施例，其中，授权认证请求中包括授权认证信息，授权认证信息中包括设备公钥，设备公钥由终端设备通过执行预定密钥生成算法生成，预定密钥生成算法的公共参数以及设备公钥被发布至公共网络，由终端设备、边缘认证节点、授权中心共享。

[0312] 授权认证模块702包括授权认证单元，用于基于设备公钥对终端设备进行授权认证。

[0313] 根据本公开的实施例，其中，终端设备通过执行预定密钥生成算法还生成设备私钥。

[0314] 授权认证单元包括获取子单元、随机数生成单元、接收子单元、签名验证子单元。

[0315] 获取子单元，用于从公共网络获取公共参数；随机数生成单元，用于根据公共参数生成第一验证随机数，将第一验证随机数发送至终端设备；接收子单元，用于接收终端设备发送的第二随机数签名信息，其中，第二随机数签名信息是由终端设备利用设备私钥对第一验证随机数进行签名生成的；签名验证子单元，用于基于公共参数，利用设备公钥对第二随机数签名信息进行验证。

[0316] 根据本公开的实施例，其中，授权认证信息中还包括授权认证请求时间戳，上述装置还包括通信时长验证模块，用于在基于设备公钥对终端设备进行授权认证之前，根据授权认证请求时间戳，验证授权认证请求的通信时长合法性。

[0317] 根据本公开的实施例，其中，令牌生成模块包括附加信息生成单元、令牌生成单元。

[0318] 其中，附加信息生成单元，用于获取令牌附加验证信息，令牌附加验证信息包括以下至少之一：终端设备的设备标识、身份令牌的令牌生成时间、身份令牌的令牌有效期；令牌生成单元，用于基于设备公钥和令牌附加验证信息生成终端设备的身份令牌。

[0319] 根据本公开的实施例，其中，授权认证信息中还包括终端设备的设备标识以及授权认证请求时间戳，附加信息生成单元包括第一生成子单元、设置子单元。

[0320] 其中，第一生成子单元，用于基于授权认证请求时间戳生成令牌生成时间；设置子单元，用于设置令牌有效期，并基于授权认证信息确定设备标识。

[0321] 根据本公开的实施例，其中，令牌生成单元包括第二生成子单元、第一组装子单元、哈希子单元、签名子单元、第二组装子单元。

[0322] 第二生成子单元，用于通过执行预定密钥生成算法生成授权中心公钥和授权中心私钥，其中授权中心公钥被发布至公共网络，由终端设备、边缘认证节点、授权中心共享；第一组装子单元，用于将设备标识、令牌生成时间、令牌有效期、设备公钥组装生成令牌摘要显性信息；哈希子单元，用于计算令牌摘要显性信息的哈希值，作为令牌摘要隐含信息；签名子单元，用于利用授权中心私钥对令牌摘要显性信息进行签名生成令牌摘要签名信息；第二组装子单元，将令牌摘要隐含信息和令牌摘要签名信息组装生成身份令牌。

[0323] 根据本公开的实施例，授权请求接收模块701、授权认证模块702、令牌生成模块703、令牌发送模块704中的任意多个模块可以合并在一个模块中实现，或者其中的任意一个模块可以被拆分成多个模块。或者，这些模块中的一个或多个模块的至少部分功能可以与其他模块的至少部分功能相结合，并在一个模块中实现。根据本公开的实施例，授权请求接收模块701、授权认证模块702、令牌生成模块703、令牌发送模块704中的至少一个可以至少被部分地实现为硬件电路，例如现场可编程门阵列(FPGA)、可编程逻辑阵列(PLA)、片上系统、基板上的系统、封装上的系统、专用集成电路(ASIC)，或可以通过对电路进行集成或封装的任何其他的合理方式等硬件或固件来实现，或以软件、硬件以及固件三种实现方式中任意一种或以其中任意几种的适当组合来实现。或者，授权请求接收模块701、授权认证模块702、令牌生成模块703、令牌发送模块704中的至少一个可以至少被部分地实现为计算机程序模块，当该计算机程序模块被运行时，可以执行相应的功能。

[0324] 基于上述接入认证方法，本公开还提供了一种接入认证装置。以下将结合图8对该装置进行详细描述。

[0325] 图8示意性示出了根据本公开实施例的接入认证装置800的结构框图。

[0326] 如图8所示，该实施例的接入认证装置800包括接入请求接收模块801、接入认证模块802。

[0327] 接入请求接收模块，用于接收终端设备发送的接入认证请求，其中，接入认证请求中包括接入认证信息，接入认证信息中包括终端设备的身份令牌，身份令牌是由授权中心对终端设备进行授权认证通过的情况下生成的；接入认证模块，用于基于接入认证请求对终端设备进行接入认证。

[0328] 根据本公开的实施例，其中，接入认证模块包括令牌认证子模块、密钥认证子模块。

[0329] 令牌认证子模块，用于对身份令牌进行令牌认证；密钥认证子模块，用于在令牌认证通过的情况下，对终端设备进行密钥认证。

[0330] 根据本公开的实施例，其中，身份令牌包括令牌摘要隐含信息和令牌摘要签名信息，其中，令牌摘要隐含信息与令牌摘要显性信息关联，令牌摘要显性信息包括终端设备的设备标识、身份令牌的令牌生成时间、身份令牌的令牌有效期、终端设备的设备公钥，令牌摘要签名信息是由授权中心利用授权中心私钥对令牌摘要显性信息进行签名生成的。

[0331] 令牌认证子模块包括第一信息获取单元、第一验签单元。

[0332] 第一信息获取单元，用于从公共网络获取授权中心公钥；第一验签单元，用于利用授权中心公钥，对令牌摘要签名信息进行验签操作。

[0333] 根据本公开的实施例,其中,验签单元包括解密子单元、匹配子单元、令牌认证子单元。

[0334] 其中,解密子单元,用于利用授权中心公钥,对令牌摘要签名信息进行解密得到参考信息;匹配子单元,用于将参考信息的哈希值与令牌摘要隐含信息进行匹配;令牌认证子单元,用于在参考信息的哈希值与令牌摘要隐含信息相匹配的情况下,通过对身份令牌的令牌认证。

[0335] 根据本公开的实施例,其中,接入认证信息中还包括终端设备的设备标识。

[0336] 上述设备还包括查询模块,用于在对身份令牌进行令牌认证之前,基于设备标识查询受信任列表,以使得在受信任列表中不包含设备标识的情况下,对身份令牌进行令牌认证。

[0337] 根据本公开的实施例,其中,接入认证信息中还包括身份令牌的令牌生成时间、身份令牌的令牌有效期。

[0338] 上述设备还包括时间戳获取模块、有效期验证模块、处理模块。

[0339] 其中,时间戳获取模块,用于在对身份令牌进行令牌认证之前,获取接入认证请求时间戳;有效期验证模块,用于基于令牌生成时间、令牌有效期、接入认证请求时间戳,对身份令牌的有效期进行验证;处理模块,用于在受信任列表中不包含设备标识,且对身份令牌的有效期验证通过的情况下,对身份令牌进行令牌认证。

[0340] 根据本公开的实施例,其中,密钥认证子模块包括挑战请求发送单元、签名信息接收单元、第二信息获取单元、第二验签单元。

[0341] 其中,挑战请求发送单元,用于向终端设备发送身份挑战请求;签名信息接收单元,用于接收由终端设备发送的第二随机数签名信息,其中,第二随机数签名信息是由终端设备响应于身份挑战请求,基于公共参数和设备私钥对第二验证随机数进行签名生成的,公共参数是由终端设备从公共网络中获得的,第二验证随机数是由终端设备随机生成的;第二信息获取单元,用于从公共网络获取公共参数和终端设备的设备公钥;第二验签单元,用于基于公共参数,利用设备公钥对第二随机数签名信息进行验证。

[0342] 根据本公开的实施例,其中,接入认证信息中包括消息随机数;上述装置还包括防攻击验证模块,用于在对终端设备进行接入认证之前,基于消息随机数对终端设备进行防攻击验证。

[0343] 根据本公开的实施例,接入请求接收模块801、接入认证模块802中的任意多个模块可以合并在一个模块中实现,或者其中的任意一个模块可以被拆分成多个模块。或者,这些模块中的一个或多个模块的至少部分功能可以与其他模块的至少部分功能相结合,并在一个模块中实现。根据本公开的实施例,接入请求接收模块801、接入认证模块802中的至少一个可以至少被部分地实现为硬件电路,例如现场可编程门阵列(FPGA)、可编程逻辑阵列(PLA)、片上系统、基板上的系统、封装上的系统、专用集成电路(ASIC),或可以通过对电路进行集成或封装的任何其他的合理方式等硬件或固件来实现,或以软件、硬件以及固件三种实现方式中任意一种或以其中任意几种的适当组合来实现。或者,接入请求接收模块801、接入认证模块802中的至少一个可以至少被部分地实现为计算机程序模块,当该计算机程序模块被运行时,可以执行相应的功能。

[0344] 图9示意性示出了根据本公开实施例的适于实现授权认证方法或接入认证方法的

电子设备的方框图。

[0345] 如图9所示，根据本公开实施例的电子设备900包括处理器901，其可以根据存储在只读存储器(ROM)902中的程序或者从存储部分908加载到随机访问存储器(RAM)903中的程序而执行各种适当的动作和处理。处理器901例如可以包括通用微处理器(例如CPU)、指令集处理器和/或相关芯片组和/或专用微处理器(例如，专用集成电路(ASIC))等等。处理器901还可以包括用于缓存用途的板载存储器。处理器901可以包括用于执行根据本公开实施例的方法流程的不同动作的单一处理单元或者是多个处理单元。

[0346] 在RAM 903中，存储有电子设备900操作所需的各种程序和数据。处理器901、ROM 902以及RAM 903通过总线904彼此相连。处理器901通过执行ROM 902和/或RAM 903中的程序来执行根据本公开实施例的方法流程的各种操作。需要注意，所述程序也可以存储在除ROM 902和RAM 903以外的一个或多个存储器中。处理器901也可以通过执行存储在所述一个或多个存储器中的程序来执行根据本公开实施例的方法流程的各种操作。

[0347] 根据本公开的实施例，电子设备900还可以包括输入/输出(I/O)接口905，输入/输出(I/O)接口905也连接至总线904。电子设备900还可以包括连接至输入/输出(I/O)接口905的以下部件中的一项或多项：包括键盘、鼠标等的输入部分906；包括诸如阴极射线管(CRT)、液晶显示器(LCD)等以及扬声器等的输出部分907；包括硬盘等的存储部分908；以及包括诸如LAN卡、调制解调器等的网络接口卡的通信部分909。通信部分909经由诸如因特网的网络执行通信处理。驱动器910也根据需要连接至输入/输出(I/O)接口905。可拆卸介质911，诸如磁盘、光盘、磁光盘、半导体存储器等等，根据需要安装在驱动器910上，以便于从其上读出的计算机程序根据需要被安装入存储部分908。

[0348] 本公开还提供了一种计算机可读存储介质，该计算机可读存储介质可以是上述实施例中描述的设备/装置/系统中所包含的；也可以是单独存在，而未装配入该设备/装置/系统中。上述计算机可读存储介质承载有一个或者多个程序，当上述一个或者多个程序被执行时，实现根据本公开实施例的方法。

[0349] 根据本公开的实施例，计算机可读存储介质可以是非易失性的计算机可读存储介质，例如可以包括但不限于：便携式计算机磁盘、硬盘、随机访问存储器(RAM)、只读存储器(ROM)、可擦式可编程只读存储器(EPROM或闪存)、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。在本公开中，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。例如，根据本公开的实施例，计算机可读存储介质可以包括上文描述的ROM 902和/或RAM 903和/或ROM 902和RAM 903以外的一个或多个存储器。

[0350] 本公开的实施例还包括一种计算机程序产品，其包括计算机程序，该计算机程序包含用于执行流程图所示的方法的程序代码。当计算机程序产品在计算机系统中运行时，该程序代码用于使计算机系统实现本公开实施例所提供的方法。

[0351] 在该计算机程序被处理器901执行时执行本公开实施例的系统/装置中限定的上述功能。根据本公开的实施例，上文描述的系统、装置、模块、单元等可以通过计算机程序模块来实现。

[0352] 在一种实施例中，该计算机程序可以依托于光存储器件、磁存储器件等有形存储介质。在另一种实施例中，该计算机程序也可以在网络介质上以信号的形式进行传输、分

发,并通过通信部分909被下载和安装,和/或从可拆卸介质911被安装。该计算机程序包含的程序代码可以用任何适当的网络介质传输,包括但不限于:无线、有线等等,或者上述的任意合适的组合。

[0353] 在这样的实施例中,该计算机程序可以通过通信部分909从网络上被下载和安装,和/或从可拆卸介质911被安装。在该计算机程序被处理器901执行时,执行本公开实施例的系统中限定的上述功能。根据本公开的实施例,上文描述的系统、设备、装置、模块、单元等可以通过计算机程序模块来实现。

[0354] 根据本公开的实施例,可以以一种或多种程序设计语言的任意组合来编写用于执行本公开实施例提供的计算机程序的程序代码,具体地,可以利用高级过程和/或面向对象的编程语言、和/或汇编/机器语言来实施这些计算程序。程序设计语言包括但不限于诸如Java,C++,python,“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设备上执行、部分地在用户设备上执行、部分在远程计算设备上执行、或者完全在远程计算设备或服务器上执行。在涉及远程计算设备的情形中,远程计算设备可以通过任意种类的网络,包括局域网(LAN)或广域网(WAN),连接到用户计算设备,或者,可以连接到外部计算设备(例如利用因特网服务提供商来通过因特网连接)。

[0355] 附图中的流程图和框图,图示了按照本公开各种实施例的系统、方法和计算机程序产品的可能实现的体系架构、功能和操作。在这点上,流程图或框图中的每个方框可以代表一个模块、程序段、或代码的一部分,上述模块、程序段、或代码的一部分包含一个或多个用于实现规定的逻辑功能的可执行指令。也应当注意,在有些作为替换的实现中,方框中所标注的功能也可以以不同于附图中所标注的顺序发生。例如,两个接连地表示的方框实际上可以基本并行地执行,它们有时也可以按相反的顺序执行,这依所涉及的功能而定。也要注意的是,框图或流程图中的每个方框、以及框图或流程图中的方框的组合,可以用执行规定的功能或操作的专用的基于硬件的系统来实现,或者可以用专用硬件与计算机指令的组合来实现。

[0356] 本领域技术人员可以理解,本公开的各个实施例和/或权利要求中记载的特征可以进行多种组合或/或结合,即使这样的组合或结合没有明确记载于本公开中。特别地,在不脱离本公开精神和教导的情况下,本公开的各个实施例和/或权利要求中记载的特征可以进行多种组合和/或结合。所有这些组合和/或结合均落入本公开的范围。

[0357] 以上对本公开的实施例进行了描述。但是,这些实施例仅仅是为了说明的目的,而并非为了限制本公开的范围。尽管在以上分别描述了各实施例,但是这并不意味着各个实施例中的措施不能有利地结合使用。本公开的范围由所附权利要求及其等同物限定。不脱离本公开的范围,本领域技术人员可以做出多种替代和修改,这些替代和修改都应落在本公开的范围之内。

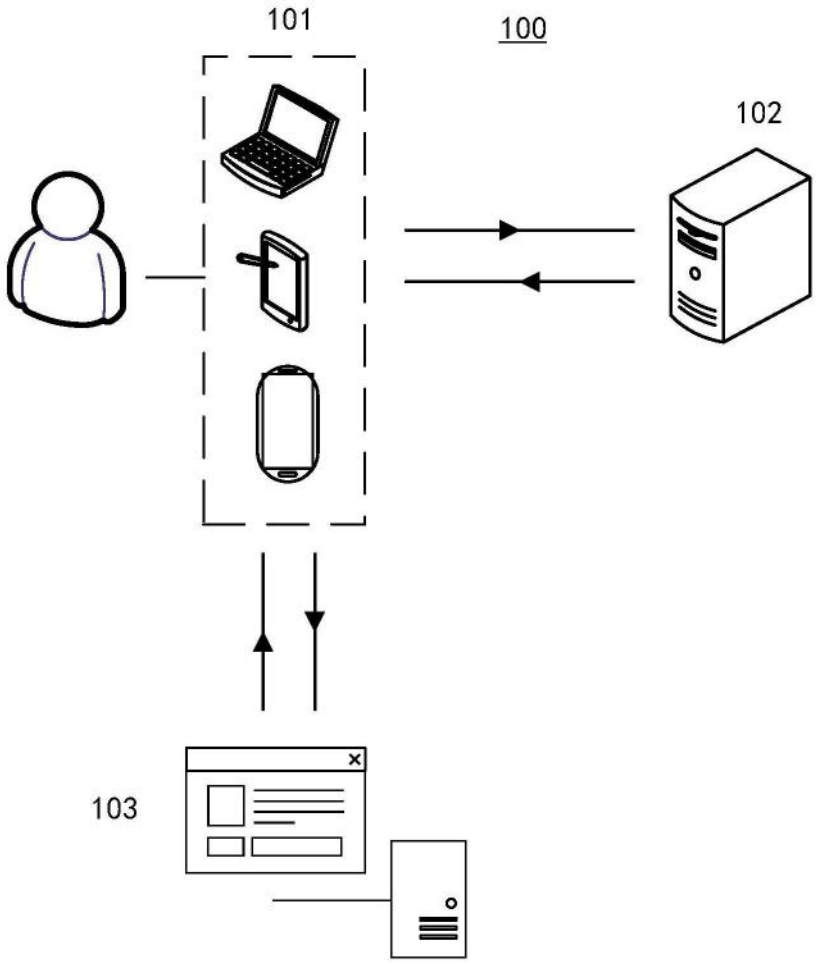


图1

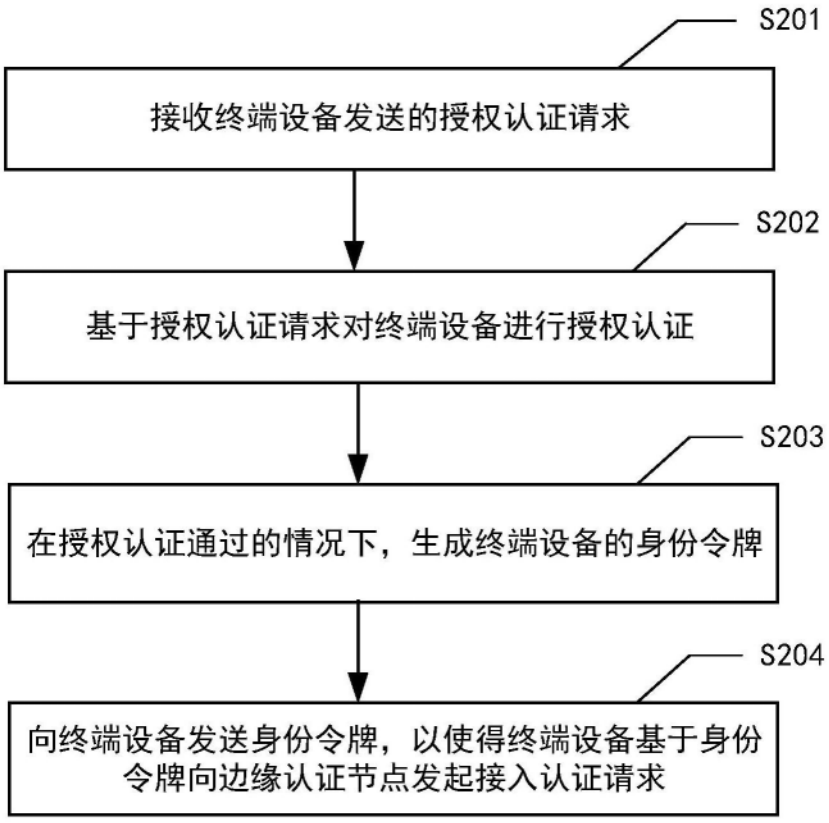

S201
接收终端设备发送的授权认证请求
S202
基于授权认证请求对终端设备进行授权认证
S203
在授权认证通过的情况下，生成终端设备的身份令牌
S204
向终端设备发送身份令牌，以使得终端设备基于身份令牌向边缘认证节点发起接入认证请求

图2

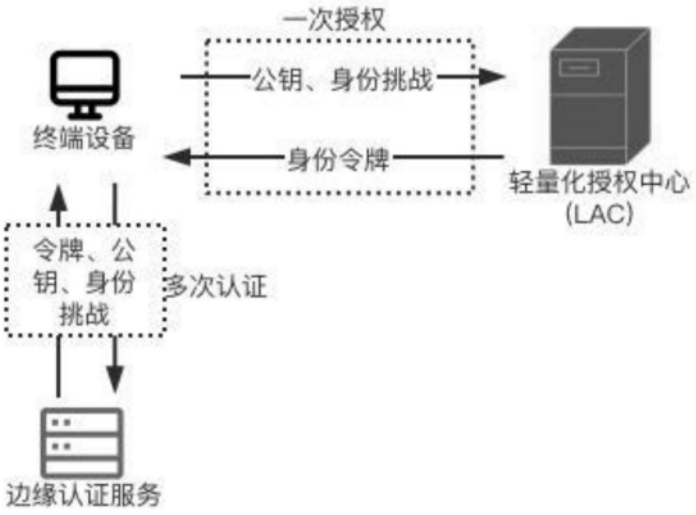

一次授权
公钥、身份挑战
身份令牌
终端设备
轻量化授权中心
(LAC)
令牌、公钥、身份挑战
多次认证
边缘认证服务

图3

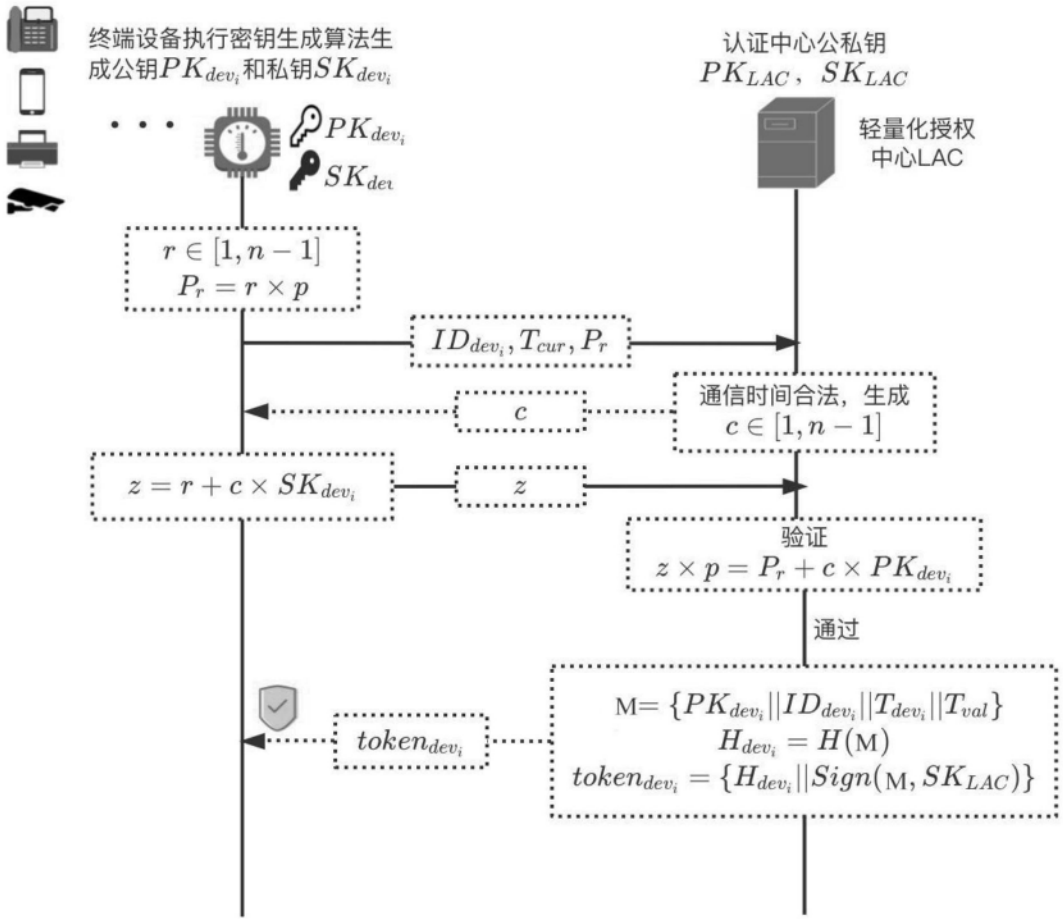

终端设备执行密钥生成算法生成公钥PK_{dev_i}和私钥SK_{dev_i}
PK_{dev_i}
SK_{dev_i}
认证中心公私钥
PK_{LAC}，SK_{LAC}
轻量化授权中心LAC
$r \in [1, n-1]$
$P_r = r \times p$
ID_{dev_i}, T_{cur}, P_r
c
通信时间合法，生成
$c \in [1, n-1]$
$z = r + c \times SK_{dev_i}$
z
验证
$z \times p = P_r + c \times PK_{dev_i}$
通过
$token_{dev_i}$
$M = \{PK_{dev_i} || ID_{dev_i} || T_{dev_i} || T_{val}\}$
$H_{dev_i} = H(M)$
$token_{dev_i} = \{H_{dev_i} || Sign(M, SK_{LAC})\}$

图4

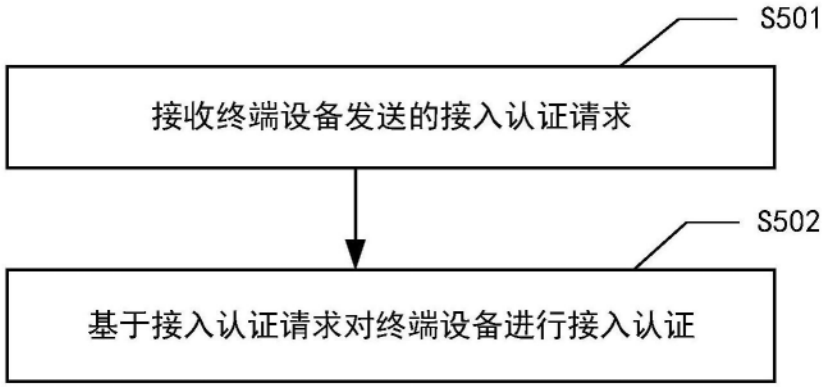

S501
接收终端设备发送的接入认证请求
S502
基于接入认证请求对终端设备进行接入认证

图5

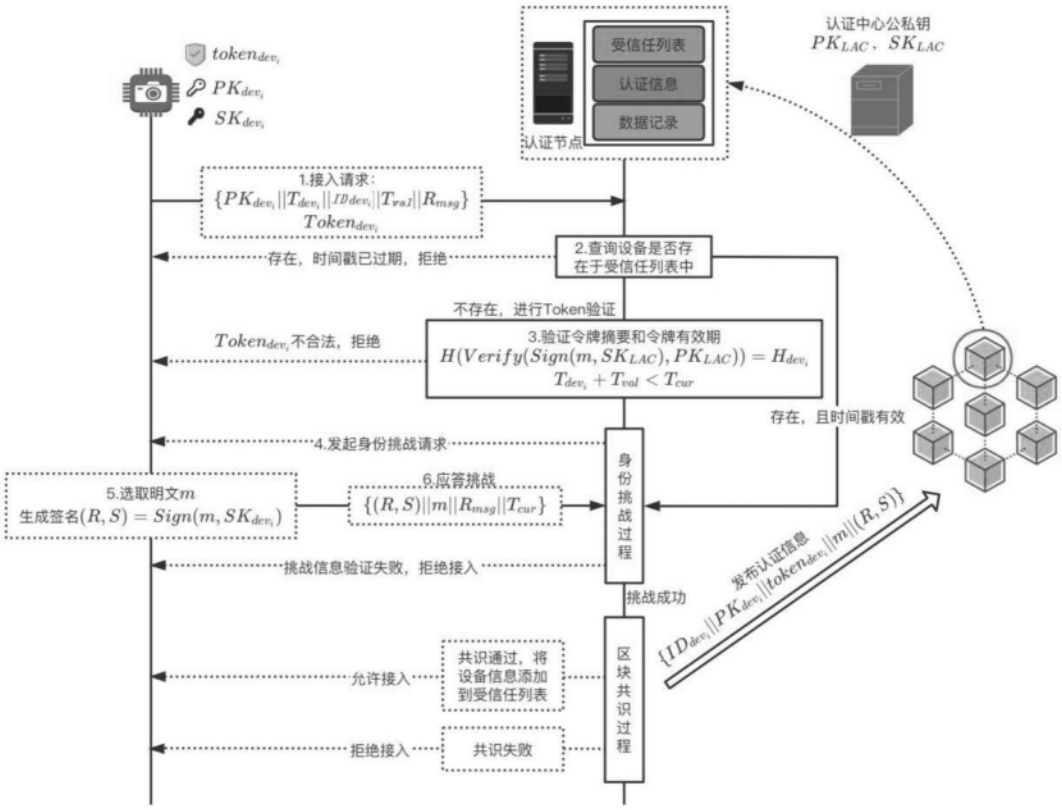

$token_{dev_i}$
PK_{dev_i}
SK_{dev_i}
受信任列表
认证信息
数据记录
认证节点
认证中心公私钥
PK_{LAC}、SK_{LAC}
1.接入请求:
$\{PK_{dev_i}||T_{dev_i}||_{IDdev_i}||T_{val}||R_{msg}\}$
$Token_{dev_i}$
存在，时间戳已过期，拒绝
2.查询设备是否存在于受信任列表中
不存在，进行Token验证
$Token_{dev_i}$不合法，拒绝
3.验证令牌摘要和令牌有效期
$H(Verify(Sign(m,SK_{LAC}),PK_{LAC}))=H_{dev_i}$
$T_{dev_i}+T_{val}<T_{cur}$
存在，且时间戳有效
4.发起身份挑战请求
5.选取明文m
生成签名$(R,S)=Sign(m,SK_{dev_i})$
6.应答挑战
$\{(R,S)||m||R_{msg}||T_{cur}\}$
身份挑战过程
挑战信息验证失败，拒绝接入
挑战成功
发布认证信息
$\{ID_{dev_i}||PK_{dev_i}||token_{dev_i}||m||(R,S)\}$
区块共识过程
允许接入
共识通过，将设备信息添加到受信任列表
拒绝接入
共识失败

图6

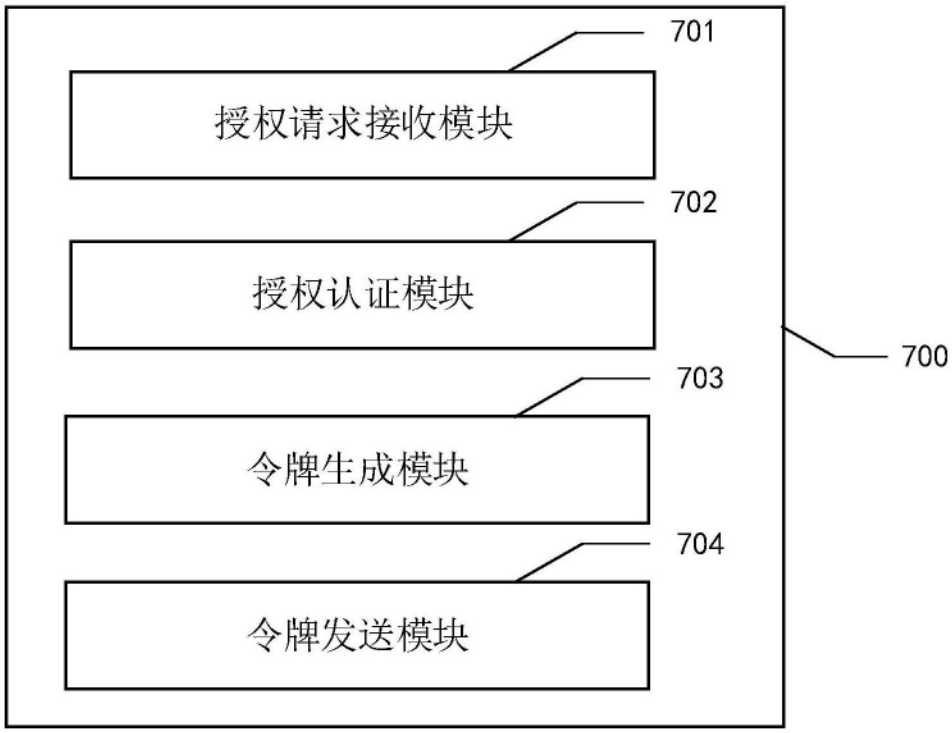

701
授权请求接收模块
702
授权认证模块
703
令牌生成模块
704
令牌发送模块
700

图7

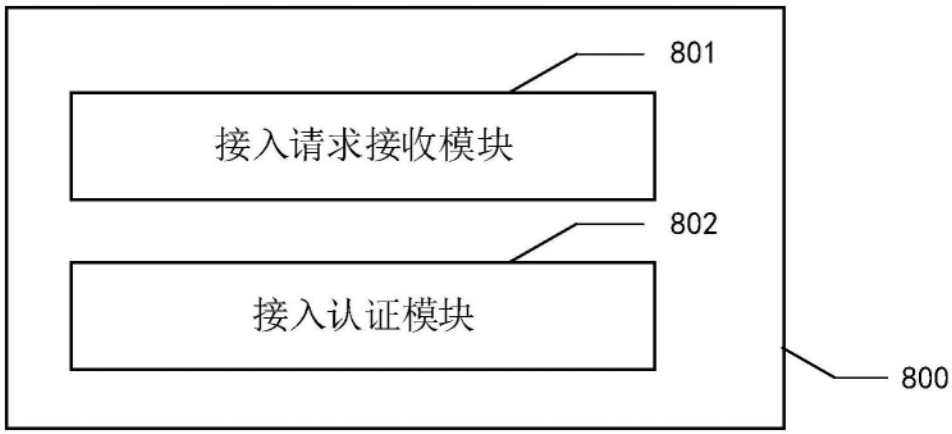

801
接入请求接收模块
802
接入认证模块
800

图8

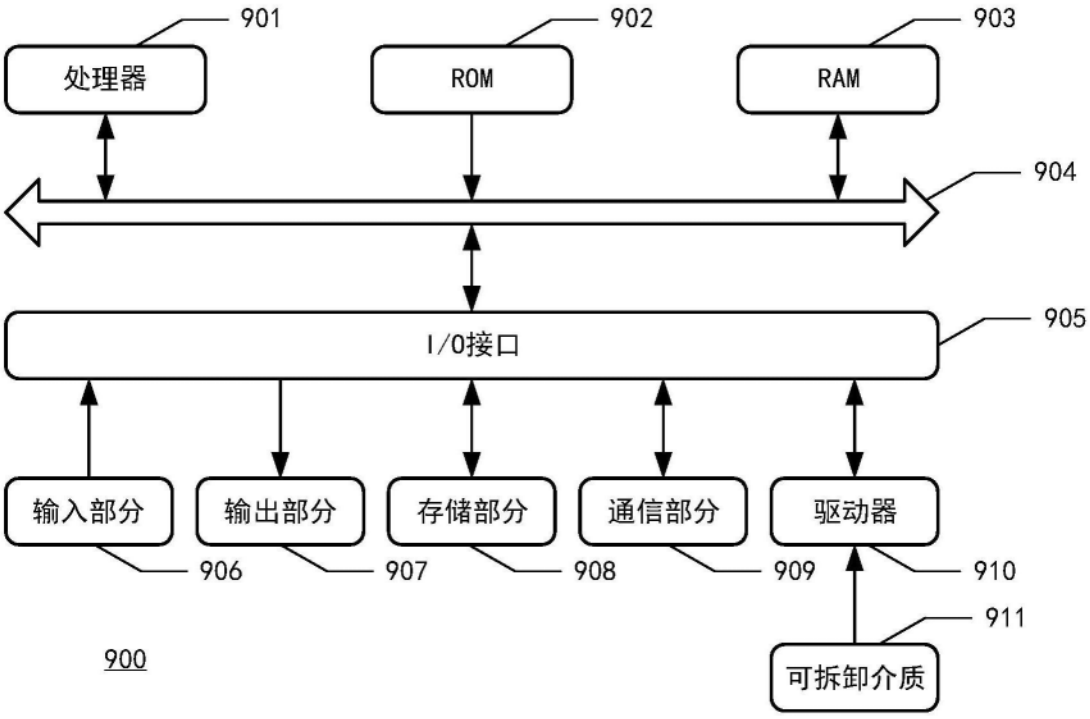

901
处理器
902
ROM
903
RAM
904
I/O接口
905
输入部分
输出部分
存储部分
通信部分
驱动器
906
907
908
909
910
911
可拆卸介质
900

图9