

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局

(43) 国际公布日
2019 年 1 月 24 日 (24.01.2019)



(10) 国际公布号
WO 2019/015500 A1

- (51) 国际专利分类号:
H04W 12/06 (2009.01) *H04W 84/12* (2009.01)
H04W 12/08 (2009.01)
- (21) 国际申请号: PCT/CN2018/094933
- (22) 国际申请日: 2018 年 7 月 9 日 (09.07.2018)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201710595977.6 2017 年 7 月 20 日 (20.07.2017) CN
- (71) 申请人: 阿里巴巴集团控股有限公司 (ALIBABA GROUP HOLDING LIMITED) [—/CN]; 开曼群岛大开曼资本大厦一座四层 847 号邮箱, Grand Cayman (KY)。
- (72) 发明人: 殷鸿展 (YIN, Hongzhan); 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。

- (74) 代理人: 北京三友知识产权代理有限公司 (BEIJING SANYOU INTELLECTUAL PROPERTY AGENCY LTD.); 中国北京市金融街 35 号国际企业大厦 A 座 16 层, Beijing 100033 (CN)。
- (81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。
- (84) 指定国 (除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM,

(54) Title: NETWORK ACCESS AUTHENTICATION METHOD, APPARATUS AND SYSTEM

(54) 发明名称: 入网认证方法、装置及系统

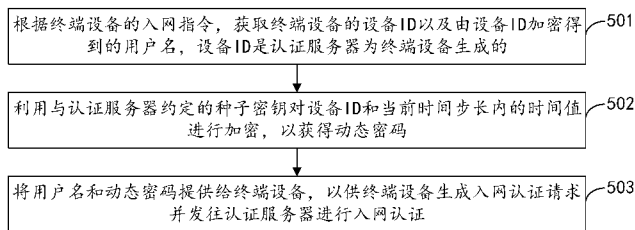


图 5

- 501 ACCORDING TO A NETWORK ACCESS INSTRUCTION FROM A TERMINAL DEVICE, ACQUIRE A DEVICE ID OF THE TERMINAL DEVICE, AND A USER NAME OBTAINED BY ENCRYPTING THE DEVICE ID, WHEREIN THE DEVICE ID IS GENERATED BY AN AUTHENTICATION SERVER FOR THE TERMINAL DEVICE
- 502 ENCRYPT THE DEVICE ID AND A TIME VALUE WITHIN THE CURRENT TIME STEP BY MEANS OF A SEED KEY AGREED WITH THE AUTHENTICATION SERVER SO AS TO OBTAIN A DYNAMIC PASSWORD
- 503 PROVIDE THE USER NAME AND THE DYNAMIC PASSWORD TO THE TERMINAL DEVICE, SUCH THAT THE TERMINAL DEVICE GENERATES A NETWORK ACCESS AUTHENTICATION REQUEST AND SENDS SAME TO THE AUTHENTICATION SERVER FOR NETWORK ACCESS AUTHENTICATION

(57) Abstract: Provided are a network access authentication method, apparatus and system. The network access authentication method mainly comprises: obtaining a user name by a network access management client encrypting a device ID of a terminal device, and obtaining a dynamic password by same encrypting the device ID and a time value within a time step, such that network access authentication is performed by the terminal device with the user name and the dynamic password. A device ID is uniquely assigned by an authentication server to a terminal device, and thus has an identity identification function for the terminal device, such that network access authentication can be independent of a digital certificate, and at the same time as network access security requirements are met, the problem of the terminal device being unable to complete network access authentication because of an unsupported or unavailable digital certificate is solved.

(57) 摘要: 本申请实施例提供一种入网认证方法、装置及系统。入网认证方法主要包括: 由入网管理客户端利用终端设备的设备ID加密得到用户名, 并利用设备ID和时间步长内的时间值加密得到动态密码, 使得终端设备以所述用户名和动态密码进行入网认证。设备ID由认证服务器为终端设备唯一分配, 所以对终端设备具有身份标识作用, 这使得入网认证可不依赖于数字证书, 在满足入网安全性需求的同时, 解决了终端设备因不支持或无法使用数字证书导致无法完成入网认证的问题。

AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布：

— 包括国际检索报告(条约第21条(3))。

入网认证方法、装置及系统

本申请要求 2017 年 07 月 20 日递交的申请号为 201710595977.6、发明名称为“入网认证方法、装置及系统”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

5

技术领域

本申请涉及网络技术领域，尤其涉及一种入网认证方法、装置及系统。

背景技术

10

随着无线局域网（Wireless Local Area Networks, WLAN）的广泛应用，为了解决 WLAN 的用户接入认证问题，出现了网络准入控制（Network Admission Control, NAC）体系。NAC 体系能够对接入 WLAN 的终端进行严格、高细粒度的管控，保证合法以及安全的终端入网，降低 WLAN 的安全风险。

15

802.1X 是 NAC 体系常用的入网认证技术。802.1X 采用的可扩展身份验证协议（Extensible Authentication Protocol, EAP）认证方式包括：EAP-MD5、EAP-PEAP、EAP-TLS、EAP-TTLS 以及 EAP-LEAP。其中，EAP-TLS 认证方式是一种基于证书的双向认证方式，其在安全性、实用性等方面都占据优势，因此成为众多企业首选的入网认证方式。

20

EAP-TLS 认证方式需要使用数字证书，来验证设备身份。但在实际场景中，特别是在终端设备一侧，经常出现不支持或无法使用数字证书等问题，造成无法完成入网认证。因此，需要一种既能兼容各种设备，又能满足设备识别、安全性等需求的入网认证方案。

发明内容

25

本申请的多个方面提供一种入网认证方法、装置及系统，用以对终端设备进行入网认证，满足设备识别、安全性等需求，同时解决设备兼容问题。

本申请实施例提供一种入网认证方法，包括：

根据终端设备的入网指令，获取所述终端设备的设备 ID 以及由所述设备 ID 加密得到的用户名，所述设备 ID 是认证服务器为所述终端设备生成的；

30

利用与所述认证服务器约定的种子密钥对所述设备 ID 和当前时间步长内的时间值进行加密，以获得动态密码；

将所述用户名和所述动态密码提供给所述终端设备，以供所述终端设备生成入网认证请求并发往所述认证服务器进行入网认证。

本申请实施例还提供一种入网认证方法，包括：

响应于入网触发操作，向入网管理客户端发送入网指令，以指示所述入网管理客户端为本端的终端设备提供入网所需的用户名和动态密码；

获取所述入网管理客户端提供的所述用户名和所述动态密码；所述用户名由所述终端设备的设备 ID 加密得到，所述动态密码由所述设备 ID 和当前时间步长内的时间值加密得到，所述设备 ID 是认证服务器为所述终端设备生成的；

根据所述用户名和所述动态密码，生成入网认证请求，并将所述入网认证请求发送给所述认证服务器，以供所述认证服务器对所述终端设备进行入网认证。

本申请实施例还提供一种入网认证方法，包括：

接收终端设备发送的入网认证请求，所述入网认证请求包括用户名和动态密码；

按照设定的解密算法，对所述用户名进行解密；

根据从所述用户名中解密出的所述终端设备的设备 ID，对所述终端设备进行可信性验证；

根据可信性验证结果、所述设备 ID 和所述入网认证请求中的动态密码，对所述终端设备进行合法性验证。

本申请实施例还提供一种电子设备，包括：存储器以及处理器；

所述存储器，用于存储程序；

所述处理器，与所述存储器耦合，用于执行所述存储器中的所述程序，以用于：

根据终端设备的入网指令，获取所述终端设备的设备 ID 以及由所述设备 ID 加密得到的用户名，所述设备 ID 是认证服务器为所述终端设备生成的；

利用与所述认证服务器约定的种子密钥对所述设备 ID 和当前时间步长内的时间值进行加密，以获得动态密码；

将所述用户名和所述动态密码提供给所述终端设备，以供所述终端设备生成入网认证请求并发往所述认证服务器进行入网认证。

本申请实施例还提供一种终端设备，包括：存储器、处理器以及通信组件；

所述存储器，用于存储程序；

所述处理器，与所述存储器耦合，用于执行所述存储器中的所述程序，以用于：

响应于入网触发操作，控制所述通信组件向入网管理客户端发送入网指令，以指示

所述入网管理客户端为所述终端设备提供入网所需的用户名和动态密码；

获取所述入网管理客户端提供的所述用户名和所述动态密码；所述用户名由所述终端设备的设备 ID 加密得到，所述动态密码由所述设备 ID 和当前时间步长内的时间值加密得到，所述设备 ID 是认证服务器为所述终端设备生成的；

- 5 根据所述用户名和所述动态密码，生成入网认证请求，并控制所述通信组件将所述入网认证请求发送给所述认证服务器，以供所述认证服务器对所述终端设备进行入网认证；

所述通信组件，用于向所述入网管理客户端发送所述入网指令，并将所述入网认证请求发送给所述认证服务器。

- 10 本申请实施例还提供一种认证服务器，包括：存储器、通信组件以及处理器；

所述存储器，用于存储程序；

所述通信组件，用于接收终端设备发送的入网认证请求，所述入网认证请求包括用户名和动态密码；

所述处理器，与所述存储器耦合，用于执行所述存储器中的所述程序，以用于：

- 15 按照设定的解密算法，对所述用户名进行解密；

根据从所述用户名中解密出的所述终端设备的设备 ID，对所述终端设备进行可信性验证；

根据可信性验证结果、所述设备 ID 和所述入网认证请求中的动态密码，对所述终端设备进行合法性验证。

- 20 本申请实施例还提供一种认证系统，包括：终端设备、入网管理客户端以及认证服务器；

所述终端设备，用于响应于入网触发操作，向所述入网管理客户端发送入网指令；获取所述入网管理客户端提供的用户名和动态密码；以及根据所述用户名和所述动态密码，生成入网认证请求，并将所述入网认证请求发送给所述认证服务器；

- 25 所述入网管理客户端，用于根据所述入网指令，获取所述设备 ID 以及所述用户名；利用与所述认证服务器约定的种子密钥对所述设备 ID 和当前时间步长内的时间值进行加密，以获得所述动态密码；以及将所述用户名和所述动态密码提供给所述终端设备；所述用户名由所述设备 ID 加密得到的；

- 所述认证服务器，用于接收所述入网认证请求，所述入网认证请求包括所述用户名
30 和所述动态密码；根据从所述用户名中解密出的所述设备 ID，对所述终端设备进行可信

性验证；以及根据可信性验证结果、所述设备 ID 和所述动态密码，对所述终端设备进行合法性验证。

在本申请实施例中，由入网管理客户端利用终端设备的设备 ID 加密得到用户名，并利用设备 ID 和时间步长内的时间值加密得到动态密码，使得终端设备以所述用户名和动态密码进行入网认证。由于设备 ID 由认证服务器为终端设备唯一分配，所以对终端设备具有身份标识作用。因此，对认证服务器来说，一方面可根据用户名中的设备 ID 识别设备身份，而无需数字证书，解决了终端设备因不支持或无法使用数字证书导致无法完成入网认证的问题，适用于各种类型的设备进行入网认证；另一方面相比于静态域密码，基于与设备 ID 相结合的动态密码进行入网认证，安全性更高，满足安全性需求。

10

附图说明

此处所说明的附图用来提供对本申请的进一步理解，构成本申请的一部分，本申请的示意性实施例及其说明用于解释本申请，并不构成对本申请的不当限定。在附图中：

图 1 为本申请一示例性实施例提供的示例性入网认证系统的结构示意图；

15 图 2 为本申请另一示例性实施例提供的入网管理客户端向认证服务器进行注册的流程图示意图；

图 3 为本申请又一示例性实施例提供的示例性入网认证系统的结构示意图；

图 4 为本申请又一示例性实施例提供的示例性入网认证方法的流程图示意图；

20 图 5 为本申请又一示例性实施例提供的从入网管理客户端的角度描述的入网认证方法的流程图示意图；

图 6 为本申请又一示例性实施例提供的从终端设备的角度描述的入网认证方法的流程图示意图；

图 7 为本申请又一示例性实施例提供的从认证服务器的角度描述的入网认证方法的流程图示意图；

25 图 8a 为本申请又一示例性实施例提供的示例性入网管理装置的结构示意图；

图 8b 为本申请又一示例性实施例提供的示例性电子设备的结构示意图；

图 9a 为本申请又一示例性实施例提供的示例性入网认证装置的结构示意图；

图 9b 为本申请又一示例性实施例提供的示例性终端设备的结构示意图；

图 10a 为本申请又一示例性实施例提供的示例性入网认证装置的结构示意图；

30 图 10b 为本申请又一示例性实施例提供的示例性认证服务器的结构示意图。

具体实施方式

为使本申请的目的、技术方案和优点更加清楚，下面将结合本申请具体实施例及相应的附图对本申请技术方案进行清楚、完整地描述。显然，所描述的实施例仅是本申请一部分实施例，而不是全部的实施例。基于本申请中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本申请保护的范围。

在现有技术中，因为 EAP-TLS 认证方式在安全性、实用性等方面的优势，成为众多企业首选的入网认证方式。但是，因为 EAP-TLS 认证方式需要使用数字证书来验证入网设备的身份，而对一些终端设备来说，经常出现不支持或无法使用数字证书等问题，造成无法完成入网认证。

针对上述技术问题，本申请实施例提供一种解决方案，主要原理是：由认证服务器为终端设备分配可唯一标识所述终端设备的设备 ID，结合入网管理客户端，由入网管理客户端为终端设备提供由终端设备的设备 ID 加密得到用户名和动态密码，终端设备以所述用户名和动态密码进行入网认证。对认证服务器来说，一方面可根据用户名中的设备 ID 识别终端设备的身份，另一方面基于与设备 ID 相结合的动态密码进行入网认证，安全性更高，满足安全性需求。

以下结合附图，详细说明本申请各实施例提供的技术方案。

图 1 为本申请一示例性实施例提供的示例性入网认证系统的结构示意图。如图 1 所示，该系统包括：终端设备 10、认证服务器 20 以及入网管理客户端 30。终端设备 10 可与认证服务器 20 以有线方式或无线方式连接。

认证服务器 20 隶属于一网络 21，主要负责其所属网络 21 的入网认证管控，确保网络 21 的安全。认证服务器 20 可以是任何可提供计算服务，能够响应服务请求，并进行处理的设备，例如可以是常规服务器、云服务器、云主机、虚拟中心等。服务器的构成主要包括处理器、硬盘、内存、系统总线等，和通用的计算机架构类似。

终端设备 10 可以是智能手机、平板电脑、个人电脑、穿戴设备等。终端设备 10 通常包括至少一个处理单元 11 和至少一个存储器 12。处理单元 11 和存储器 12 的数量取决于终端设备 10 的配置和类型。存储器 12 可以包括易失性的，例如 RAM，也可以包括非易失性的，例如只读存储器（Read-Only Memory，ROM）、闪存等，或者也可以同时包括两种类型的。存储器 12 内通常存储有操作系统（Operating System，OS）、一个或多个应用程序，也可以存储有程序数据等。除了处理单元 11 和存储器 12 之外，终端设

备还包括一些基本配置 13，例如网卡芯片、IO 总线、音视频组件等。可选地，终端设备 10 还可以包括一些外围设备 14，例如键盘、鼠标、输入笔、打印机等。这些外围设备在本领域中是总所周知的，在此不做赘述。

在本示例性的入网认证系统中，终端设备 10 可以接入认证服务器 20 所属的网络 21，但需要通过入网认证。其中，终端设备 10 主要用于根据用户名和动态密码向认证服务器 20 发起入网认证请求；入网管理客户端 30 主要用于向终端设备 10 提供入网认证所需的用户名和动态密码；认证服务器 20 主要用于根据入网认证请求对终端设备 10 进行入网认证。值得一提的是，终端设备 10 的入网操作属于系统级操作，可由终端设备的 OS 负责处理。

另外，入网管理客户端 30 可以独立于终端设备 10 实现，或者也可以安装于终端设备 10 上实现。在图 1 所示入网认证系统中，以入网管理客户端 30 安装于终端设备 10 上实现为例。如图 1 所示，当入网管理客户端 30 安装于终端设备 10 上实现时，该入网管理客户端 30 存储于存储器 12 中。终端设备 10 与入网管理客户端 30 相配合，可以实现以设备身份和动态密码进行入网认证。

当用户需要通过终端设备 10 接入认证服务器 20 所属网络 21 时，可通过终端设备 10 发出入网触发操作。例如，用户可以通过终端设备 10 上的设置选项发出入网触发操作。在一示例性的设备实现中，终端设备 10 向用户提供了设置选项，用户点击该设置选项可进入设置页面，设置页面上包括 OS 支持的各种功能设置项，例如声音、墙纸、电池、局域网/Wi-Fi、运营商等设置项。用户继续点击局域网/Wi-Fi 设置项，以进入局域网/Wi-Fi 设置页面。此时，终端设备 10 会自动搜索附近的信号强度符合设定要求的网络信息并将网络信息显示于局域网/Wi-Fi 设置页面上。在本实施例中，假设终端设备 10 搜索到的网络信息包括认证服务器 20 所属网络 21。用户通过点击局域网/Wi-Fi 设置页面上网络 21 的信息，即触发接入网络 21 的操作。

终端设备 10 可响应于入网触发操作，开始进行入网处理。终端设备 10 向入网管理客户端 30 发送入网指令，以指示入网管理客户端 30 为终端设备 10 提供入网所需的用户名和动态密码。入网管理客户端 30 接收入网指令，根据该入网指令，开始获取用户名和动态密码的操作。一方面，入网管理客户端 30 获取由认证服务器 20 为终端设备 10 生成的可唯一标识终端设备 10 的设备 ID，并获取由设备 ID 加密得到的用户名；另一方面，入网管理客户端 30 利用与认证服务器 20 约定的种子密钥对设备 ID 和当前时间步长内的时间值进行加密，以获得动态密码。因为密码生成过程与时间因子结合，所以属于动态

密码，并且该动态密码是一次性密码，每次入网都需要重新生成。

之后，入网管理客户端 30 将用户名和动态密码提供给终端设备 10。终端设备 10 获取入网管理客户端 30 提供的用户名和动态密码，根据所述用户名和动态密码，生成入网认证请求，并将入网认证请求发送给认证服务器 20，以供认证服务器 20 对终端设备 10 进行入网认证。

其中，入网管理客户端 30 可以采用多种实现方式将用户名和动态密码提供给终端设备 10。下面举例说明：

在一示例性实现方式中，在用户触发入网操作时，终端设备 10 向用户展示一入网信息页面，作为获取用户名和动态密码的途径。可选地，该入网信息页面上设置有用户名输入框和密码输入框，用户名输入框用于填充用户名，密码输入框用于填充动态密码。

可选地，对入网管理客户端 30 来说，在获取到用户名和动态密码之后，可以将用户名和动态密码填充至所述入网信息页面中，以供终端设备 10 从入网信息页面中提取所述用户名和动态密码。例如，入网管理客户端 30 可以自动将用户名填充至入网信息页面上的用户名输入框内，并将动态密码填充至入网信息页面上的密码输入框内。这种由入网管理客户端 30 自动将用户名和动态密码填充至所述入网信息页面中的实施方式，效率较高。

可选地，对入网管理客户端 30 来说，在获取到用户名和动态密码之后，也可以将用户名和动态密码输出至入网管理客户端 30 的一页面上，以供用户通过该页面获知用户名和密码。对用户来说，在触发入网操作之后，可以看到终端设备 10 提供的入网信息页面，进而获知需要输入用户名和动态密码，于是去访问入网管理客户端 30 提供的包括有用户名和动态密码的页面。对入网管理客户端 30 来说，可根据用户的访问请求，向用户展示包括有用户名和动态密码的页面，以供用户从所述页面中将用户名和动态密码复制到入网信息页面中。

当上述入网信息页面上填充用户名和动态密码后，终端设备 10 可以从该入网信息页面中获取所述用户名和动态密码，进而生成入网认证请求并发送给认证服务器 20，以供认证服务器 20 对终端设备 10 进行入网认证。

认证服务器 20 接收终端设备 10 发送的入网认证请求，该入网认证请求包括用户名和动态密码。用户名是由终端设备 10 的设备 ID 加密得到的，动态密码是利用约定的种子密钥对终端设备 10 的设备 ID 以及终端设备 10 当时指定时间步长内的时间值进行加密得到的。

之后，认证服务器 20 对用户名进行解密；若未成功解密用户名，则认证失败，拒绝终端设备 10 接入网络 21；若从用户名中成功解密出终端设备 10 的设备 ID，则根据解密出的设备 ID 对终端设备 10 进行可信性验证，因为终端设备 10 的 ID 是认证服务器 20 唯一生成的，所以基于终端设备 10 的设备 ID 可以达到识别终端设备 10 的目的。若终端设备 10 未通过可信性验证，则认证失败，拒绝终端设备 10 接入网络 21；若终端设备 10 通过可信性验证，则可以根据设备 ID 和入网认证请求中的动态密码，对终端设备 10 进行合法性验证。若终端设备 10 通过合法性验证，允许终端设备 10 接入网络 21；若终端设备 10 未通过合法性验证，拒绝终端设备 10 接入网络 21。

由上述可见，在本示例性的入网认证系统中，由入网管理客户端 30 为终端设备 10 提供由终端设备的设备 ID 加密得到用户名和动态密码，终端设备 10 以所述用户名和动态密码进行入网认证，实际上是以设备 ID 和动态密码进行入网认证。从认证服务器 20 的角度来看，一方面可根据用户名中的设备 ID 识别终端设备的身份，另一方面基于与设备 ID 相结合的动态密码进行入网认证，安全性更高，满足安全性需求。

在一示例性应用场景中，在终端设备 10 进行入网认证之前，入网管理客户端 30 可以预先向认证服务器 20 进行注册，通过该注册过程预先获得用户名、设备 ID 和种子密钥等数据。如图 2 所示，一种入网管理客户端 30 向认证服务器 20 进行注册的流程包括以下步骤：

201、入网管理客户端 30 向认证服务器 20 发送注册请求，所述注册请求携带有终端设备 10 的硬件信息。

此处不对硬件信息进行限定，凡是与终端设备 10 相关的硬件信息均适用于本实施例，例如可以是与终端设备 10 的中央处理单元（Central Processing Unit, CPU）、显卡、硬盘等相关的信息。

可选地，注册请求中还可以包括终端设备 10 对应的用户信息和/或企业信息。

202、认证服务器 20 接收注册请求，从中解析出终端设备 10 的硬件信息，并根据所述硬件信息生成可唯一标识终端设备 10 的设备 ID，记为 UMID。

可选地，当注册请求中包括用户信息和/或企业信息时，认证服务器 20 可以存储终端设备 10 对应的用户信息和/或企业信息，并且还可以根据该用户信息和/或企业信息为终端设备生成用户 ID（User ID, UID）和/或企业 ID（Customer Identity, CID）。其中，UID 用于唯一标识终端设备 10 所属的用户；CID 用户唯一标识终端设备 10 所属的企业。

例如，用户信息可以包括但不限于：用户注册的账号、密码、用户的邮箱、手机号码、昵称等信息。企业信息可以包括但不限于：用户注册的账号、密码、企业注册地、企业名称、企业性质、企业规模等信息。

203、认证服务器 20 采用设定的加密算法生成两个动态令牌（token），即令牌密钥（TokenKey，TK）和进程令牌（ProcessToken，PT）。

其中，TK 可作为终端设备 10 入网认证时所需的用户名，由 UMID 加密得到。PT 可作为加密后的种子密钥，可由 UMID、TK 以及种子密钥加密得到。

可选地，可以采用 Blowfish 加密算法对 UMID 进行加密以生成 TK。

可选地，可以采用 AES-128 加密算法对 UMID、TK 以及种子密钥加密以生成 PT。

10 进一步，当认证服务器 20 为终端设备生成 CID、UID 和 UMID 时，可以同时结合 CID、UID 和 UMID 来生成 TK 和 PT。其中，结合 CID、UID 和 UMID 生成 TK 和 PT 的加密公式分别如下：

$$TK = \text{Blowfish}(\text{CID} + \text{UID} + \text{UMID} + \text{RANDOM} + \text{TIME}, (\text{app_secret}))$$

$$PT = \text{TK} + \text{AES128}(\text{CID} + \text{UID} + \text{UMID}, (\text{app_secret}))$$

15 在上述加密公式中，app_secret 表示入网管理客户端 30 与认证服务器 20 约定的种子密钥。该种子密钥可以是入网管理客户端 30 的 API 接口密钥，与入网管理客户端 30 一一对应。

204、认证服务器向入网管理客户端 30 发送 TK、PT 以及 UMID。

20 205、入网管理客户端 30 接收 TK、PT 以及 UMID，并将 UMID、TK 保存在本地空间中。

206、入网管理客户端 30 向独立的加密工具发送 PT，由加密工具对 PT 解密获得种子密钥并存储种子密钥。

25 其中，加密工具对入网管理客户端 30 以及认证服务器 20 来说是一个黑匣子，其采用的加密算法以及存储种子密钥的方式对外不可见，且加密工具具有防篡改功能，而且在不安全的情况下禁止被访问或使用，这样可以降低种子密钥被破解的风险，保证种子密钥的安全性，进而可提高入网认证的安全性。对入网管理客户端 30 和认证服务器来说，在需要时只需调用加密工具即可。

30 基于上述注册流程，入网管理客户端 30 可以预先将终端设备 10 的设备 ID 和用户名保存至本地空间中。因此，当接收到入网指令时，入网管理客户端 30 可直接从本地空间中读取终端设备 10 的设备 ID 和用户名。除该实施方式之外，入网管理客户端 30 也可以

在接收到入网指令时，实时地向认证服务器 20 请求终端设备 10 的设备 ID 和用户名。例如，如果认证服务器 20 未在上述注册流程中向入网管理客户端 30 下发终端设备 10 的设备 ID 和用户名，则入网管理客户端 30 在接收到入网指令时，需要实时地向认证服务器 20 请求终端设备 10 的设备 ID 和用户名。其中，由认证服务器 20 向入网管理客户端 30 5 下发终端设备 10 的设备 ID 和用户名，加密算法只需保存在认证服务器 20 一端，有利于降低加密算法被破解的概率，进而提高设备 ID 和用户名的安全性。

进一步可选地，在上述注册流程中，认证服务器 20 可以通过注册设备列表存储已注册设备的设备 ID，并通过设备状态列表存储已注册设备的状态，例如已注册、已删除、10 被冻结、被禁用等。其中，注册设备列表和设备状态列表可以是同一列表，也可以是相互独立的两个列表。

基于上述注册设备列表和设备状态列表，认证服务器 20 可以结合注册设备列表和设备状态列表，对终端设备 10 进行可信性验证。一种可选实施方式包括：当从用户名中成功解密出终端设备 10 的设备 ID 时，认证服务器 20 根据解密出的设备 ID 查找注册设备15 列表，以判断终端设备 10 是否已经注册；如果从注册设备列表中查询到所述解密出的设备 ID，进一步查询设备状态列表，以判断终端设备 10 的状态是否正常；如果从设备状态列表中查询到终端设备 10 处于正常状态，确定终端设备 10 通过可信性验证。如果未从注册设备列表中查询到所述解密出的设备 ID，或者从设备状态列表中查询到终端设备10 处于异常状态，例如被删除、被禁用、被冻结，则确定终端设备 10 未通过可信性验证。20

在一可选实施方式中，认证服务器 20 在生成用户名（即 TK）的过程可以同时结合 CID 和/或 UID。基于此，认证服务器 20 除了可以从用户名中解密出 UMID 之外，还可以从用户名中解密出 UID 和/或 CID。为了提高网络安全性，可以从设备角度、用户角度以及企业角度进行多因素认证。基于此，认证服务器 20 在对终端设备 10 进行可信性验证之前，可以根据 UID 和预先注册的用户信息和/或企业信息，对终端设备 10 所属的用户和/或企业进行身份验证；例如，可以判断从用户名中解密出的 UID 和/或 CID 是否与25 预先注册的用户信息和/或企业信息相匹配，如果相匹配，确定终端设备 10 所属的用户和/或企业通过身份验证；如果不匹配，确定终端设备 10 所属的用户和/或企业未通过身份验证。当终端设备 10 所属的用户和/或企业通过身份验证时，再对终端设备 10 进行可信性验证。30

在上述实施例或下述实施例中，在终端设备 10 通过可信性验证之后，认证服务器 20 需要根据设备 ID 和入网认证请求中的动态密码对终端设备 10 进行合法性验证。

一种对终端设备 10 进行合法性验证的实施方式包括：认证服务器 20 可以确定至少
5 两个时间步长，其中，所述至少两个时间步长包括当前时间步长以及与当前时间步长相
距最近的至少一个历史时间步长；对至少两个时间步长中的每个时间步长，利用与入网
管理客户端 30 约定的种子密钥对解密出的设备 ID 和每个时间步长内的时间值进行加密，
以生成至少两个动态密码；根据至少两个动态密码和入网认证请求中的动态密码，对终
端设备进行合法性验证。例如，可以将至少两个动态密码与入网认证请求中携带的动态
10 密码进行比较；若至少两个动态密码中存在与入网认证请求中携带的动态密码相同的动
态密码，则确定终端设备 10 通过合法性验证；若至少两个动态密码中不存在与入网认
证请求中携带的动态密码相同的动态密码，则确定终端设备 10 未通过合法性验证。

进一步可选地，认证服务器 20 可以存储已认证设备的映射数据。这里已认证设备包
括当前在线的已认证设备，也包括已下线的历史已认证设备。已认证设备的映射数据包
15 括但不限于：已认证设备的设备 ID、媒体访问控制（Media Access Control, MAC）地址、
UID、CID、认证通过时所使用的动态密码等数据。基于此，认证服务器 20 可以结合已
认证设备的映射数据对终端设备进行合法性验证。

另一种对终端设备 10 进行合法性验证的实施方式包括：认证服务器 20 根据从用户
名中解密出的设备 ID 判断已认证设备的映射数据中是否存在终端设备上上次认证通过所
20 使用的动态密码。若已认证设备的映射数据中存在终端设备上上次认证通过所使用的动
态密码，则根据终端设备上上次认证通过所使用的动态密码和入网认证请求中携带的动态
密码，对终端设备 10 进行合法性验证。例如，可以将终端设备上上次认证通过所使用的动
态密码与入网认证请求中携带的动态密码进行比较；若两者相同，则确定终端设备 10 通
过合法性验证；若两者不相同，则确定终端设备 10 未通过合法性验证。

25 若已认证设备的映射数据中不存在终端设备上上次认证通过所使用的动态密码，则认
证服务器 20 确定至少两个时间步长，利用与入网管理客户端 30 约定的种子密钥分别对
设备 ID 和每个时间步长内的时间值进行加密，以获得至少两个动态密码；将至少两个动
态密码与入网认证请求中携带的动态密码进行比较；若至少两个动态密码中存在与入网
认证请求中携带的动态密码相同的动态密码，则确定终端设备 10 通过合法性验证；若至
30 少两个动态密码中不存在与入网认证请求中携带的动态密码相同的动态密码，则确定终

端设备 10 未通过合法性验证。

可选地，在上述认证过程中，认证服务器 20 也可以将设备 ID 以及当前时间步长或历史时间步长内的时间值发送给加密工具，以使加密工具利用预先约定的种子密钥对设备 ID 以及当前时间步长或历史时间步长内的时间值进行加密，从而获得动态密钥。

5 值得说明的是，动态密码具有一定时效性，当时效性结束时，该动态密码就会失效，故会被删除。在同一个时间步长内，动态密码生成的结果是一样的。对认证服务器 20 来说，并不知道入网认证请求中携带的动态密码是在哪个时间步长内生成的，而且由于网络的原因，动态密码生成端（即入网管理客户端 30）的时间和认证服务器 20 接收到动态密码的时间可能差距会很大，有可能使得这两个时间不在同一个时间步长内。例如，
10 可能存在这种情况：入网管理客户端 30 在一个时间步长的结尾时刻生成动态密码，认证服务器 20 在下一个时间步长的开始时刻接收到该动态密码，这种情况属于合理情况。基于此，考虑到传输时延，在上述计算动态密码的过程中不仅考虑当前时间步长，而且考虑与当前时间步长相邻的历史时间步长，历史时间步长可以是一个或多个。历史时间步长的个数越多，被攻击的风险就越大，因此历史时间步长的个数可视网络的风险容忍程
15 度而定。

进一步，认证服务器 20 在获得终端设备 10 的认证结果之后，还可以向终端设备 10 返回认证结果。所述认证结果包括：终端设备 10 通过认证，或终端设备 10 未通过认证。

图 1 所示入网认证系统可在 802.1X 协议框架下部署实施。可选地，图 1 所示入网认证系统还可与 802.1X 协议中的 EAP-PEAP 认证方式相结合，以 EAP-PEAP 作为载体形成一种新的认证方式，但并不限于与 EAP-PEAP 认证方式相结合。基于此，如图 3 所示，另一种示例性的入网认证系统主要包括：终端设备 10、认证服务器 20、入网管理客户端 30、Radius 服务器 40 以及网络附属存储（Network Attached Storage，NAS）设备 50。终端设备 10 通过 NAS 设备 50 与 Radius 服务器 40 连接，Radius 服务器 40 与认证服
20 器 20 连接。
25

值得说明的是，图 3 所示入网认证系统中，除了终端设备 10、NAS 设备 50、Radius 服务器 30 以及认证服务器 20 之外，还可以包括网关等其它一些网络设备，在此不做赘述，具体可视网络部署情况而定。

在图 3 所示示例性的入网认证系统中，终端设备 10、认证服务器 20 以及入网管理
30 客户端 30 的功能基本不变。终端设备 10 仍旧主要用于根据用户名和动态密码向认证服

务器 20 发起入网认证请求，发起过程参见前面的描述；入网管理客户端 30 仍旧主要用于向终端设备 10 提供入网认证所需的用户名和动态密码；认证服务器 20 仍旧主要用于对终端设备 10 进行入网认证，认证过程参见前面的描述。区别在于：终端设备 10 与认证服务器 20 之间的交互数据需要封装为远程用户拨号认证系统（Remote authentication dial in user service, Radius）协议报文，并通过 Radius 服务器 40 进行转发。

Radius 是一种客户端/服务器（C/S）结构的协议，Radius 服务器 40 和 NAS 设备 50 分别是 Radius 协议下的服务器和客户端。其中，NAS 设备 50 可以是任何运行 Radius 客户端软件的设备，主要向远程接入用户（即终端设备 10）提供接入及与 Radius 服务器 40 交互的服务。在本实施例中，Radius 服务器 40 主要作为认证服务器 20 的代理，负责 Radius 协议报文的封装/解封装以及转发，这点不同于传统意义上的 Radius 服务器。其中，Radius 服务器 40 可以是任何运行 Radius 服务端软件的设备。

在图 3 所示入网认证系统中，终端设备 10 可以采用图 2 所示流程向认证服务器 20 进行注册，详细流程在此不再赘述。之后，当用户需要通过终端设备 10 接入认证服务器 20 所属的网络 21 时，可进入入网认证流程。可选地，如图 4 所示，可在图 3 所示入网认证系统中实施的一种认证流程包括以下步骤：

认证初始化阶段：

401、终端设备 10 响应于用户触发的入网操作，向入网管理客户端 30 发送入网指令，与此同时，在终端设备的界面上展示入网信息页面。

402、入网管理客户端 30 可从本地空间中读取 UMID 以及 TK，将 TK 作为用户名。

403、入网管理客户端 30 调用加密工具，由加密工具利用种子密钥对 UMID 和当前时间步长内的时间值进行加密，以获得动态密码。

可选地，时间步长可以是 5 分钟、3 分钟、2 分钟等，具体视应用需求而定。

404、入网管理客户端 30 自动将 TK 和动态密码填充至入网信息页面上。

405、终端设备 10 从入网信息页面中获取 TK 和动态密码。

传输层安全（Transport Layer Security, TLS）通道建立阶段：

406、终端设备 10 向 NAS 设备 50 发送一个 EAPoL-Start 报文，开始 802.1X 接入的开始。

407、NAS 设备 50 向终端设备 10 发送 EAP-Request/Identity 报文，要求终端设备 10 上报用户的网络标识。

408、终端设备 10 向 NAS 设备 50 回应一个 EAP-Response/Identity 报文。

409、NAS 设备 50 以 EAPoR (EAP over Radius) 的报文格式将 EAP-Response/Identity 发送给 Radius 服务器 40。

410、Radius 服务器 40 收到 EAP-Response/Identity 报文, 根据配置确定使用 EAP-PEAP 认证, 并向 NAS 设备 50 发送 RADIUS-Access-Challenge 报文, 该报文里面含有 Radius 服务器 40 发送给终端设备 10 的 EAP-Request/Peap/Start 报文, 表示希望开始进行 EAP-PEAP 的认证。

411、NAS 设备 50 将 EAP-Request/Peap/Start 报文发送给终端设备 10。

改进 MSCHPAV2 认证阶段:

412、终端设备 10 收到 EAP-Request/Peap/Start 报文后, 按照 MSCHPAV2 算法对动态密码进行处理, 获得一哈希值, 记为 ntSendResponse, 将用户名和哈希值 ntSendResponse, 封装在 EAP-Response/Client Hello 报文中发送给 NAS 设备 50。

413、NAS 设备 50 以 EAPoR 的报文格式将 EAP-Response/Client Hello 报文发送给 Radius 服务器 40。

414、Radius 服务器 40 收到终端设备 10 发来的 EAP-Response/Client Hello 报文后, 从中解析出 TK 和哈希值 ntSendResponse。

415、Radius 服务器 40 向认证服务器 20 发送 TK 和哈希值 ntSendResponse。

416、认证服务器 20 按照设定的解密算法对用户名进行解密; 若成功解密, 进入步骤 417; 若未成功解密, 进入步骤 421。该解密算法与认证服务器 20 在注册流程中生成用户名时采用的加密算法相对应。

417、认证服务器 20 根据从用户名中解密出的设备 ID 对终端设备 10 进行可信性验证; 若终端设备 10 通过可信性验证, 进入步骤 418; 若未通过可信性验证, 进入步骤 421。

418、认证服务器 20 根据设备 ID 和哈希值 ntSendResponse, 对终端设备 10 进行合法性验证; 若通过合法性验证, 进入步骤 419; 若未通过合法性验证, 进入步骤 421。

在本实施例中, 认证服务器 20 会记录已认证设备的映射数据。已认证设备的映射数据中包括已认证设备的设备 ID、MAC 地址、用户名、哈希值以及认证过程中所需的哈希密码等信息。基于此, 认证服务器 20 可以根据设备 ID 判断已认证设备的映射数据中是否存在终端设备 10 上一次通过认证所使用的哈希密码。

若判断结果为存在, 则对终端设备 10 上一次通过认证所使用的哈希密码做哈希处理得到一哈希值; 将该哈希值与哈希值 ntSendResponse 进行比较; 两个哈希值相同, 确定终端设备 10 通过合法性验证; 若两个哈希值不相同, 确定终端设备 10 未通过合法性验证。

证。

若判断结果为不存在，根据当前时间，确定当前时间步长以及与当前时间步长相邻的历史时间步长；利用与入网管理客户端 30 约定的种子密钥对设备 ID 和所确定的每个时间步长内的时间值进行加密，获得至少两个动态密码；按照 MSCHPAV2 算法对至少两个动态密码进行处理，获得至少两个哈希密码；进而，对至少两个哈希密码进行哈希处理，获得至少两个哈希值。将至少两个哈希值与哈希值 ntSendResponse 进行比较；若至少两个哈希值中存在与哈希值 ntSendResponse 相同的哈希值，确定终端设备 10 通过合法性验证；若至少两个哈希值中不存在与哈希值 ntSendResponse 相同的哈希值，确定终端设备 10 未通过合法性验证。

当确定终端设备 10 通过合法性验证后，将与哈希值 ntSendResponse 相同的哈希值所对应的哈希密码存储到终端设备 10 的映射数据中。

419、认证服务器 20 通过 MSCHPAV2 算法生成一个认证通过标识 msch_response，并向 Radius 服务器 40 发送认证通过标识 msch_response。

420、Radius 服务器 40 将认证通过标识 msch_response 封装在 RADIUS-Access-Accept 报文中，通过 NAS 设备 50 向终端设备 10 发送 RADIUS-Access-Accept 报文，结束认证流程。

421、认证服务器 20 向 Radius 服务器 40 发送未通过认证结果，并进入步骤 422。

422、Radius 服务器 40 将未通过认证结果封装在 RADIUS-Access-Reject 报文中，并通过 NAS 设备 50 向终端设备 10 发送 RADIUS-Access-Reject 报文，结束认证流程。

基于上述图 1 或图 3 所示的入网认证系统，本申请以下实施例分别从入网管理客户端、终端设备以及认证服务器的角度给出了几种入网认证方法的流程。

从入网管理客户端的角度来看，一种入网认证方法的流程如图 5 所示，包括以下步骤：

501、根据终端设备的入网指令，获取终端设备的设备 ID 以及由设备 ID 加密得到的用户名，设备 ID 是认证服务器为终端设备生成的。

502、利用与认证服务器约定的种子密钥对设备 ID 和当前时间步长内的时间值进行加密，以获得动态密码。

503、将用户名和动态密码提供给终端设备，以供终端设备生成入网认证请求并发往认证服务器进行入网认证。

在一可选实施方式中，上述将用户名和动态密码提供给终端设备，包括：

将用户名和动态密码填充至终端设备提供的入网信息页面中；或者

将用户名和动态密码输出至本端页面上，并根据用户的访问请求，向用户展示本端页面，以供用户从本端页面中将用户名和动态密码复制到终端设备提供的入网信息页面中。

在一可选实施方式中，上述种子密钥由独立于本端的加密工具维护管理。基于此，上述利用与认证服务器约定的种子密钥对设备 ID 和当前时间步长内的时间值进行加密，以获得动态密码，包括：将设备 ID 和当前时间步长内的时间值发送给加密工具，以使加密工具利用种子密钥对设备 ID 和当前时间步长内的时间值进行加密并输出动态密码。

在一可选实施方式中，在根据终端设备的入网指令，获取终端设备的设备 ID 以及由设备 ID 加密得到的用户名之前，还可以向认证服务器进行注册。在所述注册流程中，入网管理客户端主要执行以下操作：向认证服务器发送注册请求，所述注册请求包括终端设备的硬件信息，所述硬件信息用于供认证服务器为终端设备生成设备 ID；接收认证服务器下发的用户名、设备 ID 以及由用户名和设备 ID 加密后的种子密钥；将设备 ID 以及用户名存储在本地空间中，并将由用户名和设备 ID 加密后的种子密钥发送至加密工具，以供加密工具解密出种子密钥。

在一可选实施方式中，上述注册请求还包括：终端设备对应的用户信息；所述用户信息用于供认证服务器为终端设备生成用户 ID。基于此，入网管理客户端还会接收认证服务器下发的用户 ID。

从终端设备的角度来看，一种入网认证方法的流程如图 6 所示，包括以下步骤：

601、响应于入网触发操作，向入网管理客户端发送入网指令，以指示入网管理客户端为本端的终端设备提供入网所需的用户名和动态密码。

602、获取入网管理客户端提供的用户名和动态密码；用户名由终端设备的设备 ID 加密得到，动态密码由设备 ID 和当前时间步长内的时间值加密得到，设备 ID 是认证服务器为终端设备生成的。

603、根据用户名和动态密码，生成入网认证请求，并将入网认证请求发送给认证服务器，以供认证服务器对终端设备进行入网认证。

在一可选实施方式中，在响应入网触发操作时，还可以向用户展示一入网信息页面，以获取用户名和动态密码。基于此，上述获取入网管理客户端提供的用户名和动态密码，

包括：从所述入网信息页面中获取用户名和动态密码。其中，用户名和动态密码是由入网管理客户端填充至入网信息页面中，或者由用户从入网管理客户端的页面中复制到入网信息页面中。

5 从认证服务器的角度来看，一种入网认证方法的流程如图 7 所示，包括以下步骤：

701、接收终端设备发送的入网认证请求，入网认证请求包括用户名和动态密码。

702、按照设定的加密算法，对所述用户名进行解密。

703、根据从用户名中解密出的终端设备的设备 ID，对终端设备进行可信性验证。

704、根据可信性验证结果、设备 ID 和入网认证请求中的动态密码，对终端设备进行合法性验证。
10

在一可选实施方式中，上述根据从用户名中解密出的终端设备的设备 ID，对终端设备进行可信性验证，包括：当从用户名成功解密出终端设备的设备 ID 时，根据设备 ID 查找注册设备列表，注册设备列表存储有已注册设备的设备 ID；从注册设备列表中查询到设备 ID，查询设备状态列表，设备状态列表存储有已注册设备的状态；若从设备状态
15 列表中查询到终端设备处于正常状态，确定终端设备通过可信性验证。

在一可选实施方式中，上述用户名中还包括：终端设备对应的用户 ID。基于此，在根据设备 ID 对终端设备进行可信性验证之前，还可以根据用户 ID 和预先注册的终端设备对应的用户信息，对终端设备所属的用户进行合法性验证；当终端设备所属的用户通过合法性验证时，执行根据设备 ID 对终端设备进行可信性验证的操作。

20 在一可选实施方式中，上述根据可信性验证结果、设备 ID 和入网认证请求中的动态密码，对终端设备进行合法性验证，包括：当终端设备通过可信性验证时，利用与入网管理客户端约定的种子密钥分别对设备 ID 和至少两个时间步长中每个时间步长内的时间值进行加密，以生成至少两个动态密码；根据至少两个动态密码和入网认证请求中的动态密码，对终端设备进行合法性验证；其中，至少两个时间步长包括当前时间步长以及
25 与当前时间步长相距最近的至少一个历史时间步长。

在一可选实施方式中，上述在利用与入网管理客户端约定的种子密钥分别对设备 ID 和至少两个时间步长中每个时间步长内的时间值进行加密，以获得至少两个动态密码之前，还可以根据设备 ID 判断已认证设备的映射数据中是否存在终端设备上次认证通过所使用的动态密码；若判断结果为存在，根据终端设备上次认证通过所使用的动态密码和
30 入网认证请求中的动态密码，对终端设备进行合法性验证；若判断结果为不存在，执行

利用与入网管理客户端约定的种子密钥分别对设备 ID 和至少两个时间步长中每个时间步长内的时间值进行加密，以生成至少两个动态密码的操作。

在一可选实施方式中，上述在接收终端设备发送的入网认证请求之前，还包括一注册流程。在所述注册流程中，认证服务器主要执行以下操作：接收入网管理客户端发送的注册请求，所述注册请求携带有终端设备的硬件信息；根据所述注册请求中的硬件信息为终端设备生成设备 ID；对所述设备 ID 进行加密，以生成用户名；利用用户名和设备 ID 对种子密钥进行加密，以获得加密后的种子密钥；将用户名、设备 ID 以及加密后的种子密钥发送给入网管理客户端。

需要说明的是，上述实施例所提供方法的各步骤的执行主体均可以是同一设备，或者，该方法也由不同设备作为执行主体。比如，步骤 501 至步骤 503 的执行主体可以为设备 A；又比如，步骤 501 和 502 的执行主体可以为设备 A，步骤 503 的执行主体可以为设备 B；等等。

图 8a 为本申请又一实施例提供的入网管理装置的结构示意图。该入网管理装置可作为前述的入网管理客户端实现。如图 8a 所示，所述入网管理装置包括：获取模块 81、加密模块 82 和提供模块 83。

获取模块 81，用于根据终端设备的入网指令，获取所述终端设备的设备 ID 以及由所述设备 ID 加密得到的用户名，所述设备 ID 是认证服务器为所述终端设备生成的。

加密模块 82，用于利用与所述认证服务器约定的种子密钥对所述设备 ID 和当前时间步长内的时间值进行加密，以获得动态密码。

提供模块 83，用于将所述用户名和所述动态密码提供给所述终端设备，以供所述终端设备生成入网认证请求并发往所述认证服务器进行入网认证。

在一可选实施方式中，提供模块 83 具体用于：将所述用户名和所述动态密码填充至所述终端设备提供的入网信息页面中；或者，将所述用户名和所述动态密码输出至本端页面上，并根据用户的访问请求，向所述用户展示所述本端页面，以供所述用户从所述本端页面中将所述用户名和所述动态密码复制到所述终端设备提供的入网信息页面中。

在一可选实施方式中，种子密钥由独立于本端的加密工具维护管理。基于此，加密模块 82 具体用于：将所述设备 ID 和当前时间步长内的时间值发送给所述加密工具，以使所述加密工具利用所述种子密钥对所述设备 ID 和当前时间步长内的时间值进行加密并输出所述动态密码。

在一可选实施方式中，入网管理装置还包括：发送模块、接收模块和存储模块。

发送模块，向所述认证服务器发送注册请求，所述注册请求包括所述终端设备的硬件信息，所述硬件信息用于供所述认证服务器为所述终端设备生成所述设备 ID。

接收模块，用于接收所述认证服务器下发的所述用户名、所述设备 ID 以及由所述用户名和所述设备 ID 加密后的种子密钥。

5 存储模块，用于将所述设备 ID 以及所述用户名存储在本地空间中，并将由所述用户名和所述设备 ID 加密后的种子密钥发送至所述加密工具，以供所述加密工具解密出所述种子密钥。

在一可选实施方式中，所述注册请求还包括：所述终端设备对应的用户信息；所述用户信息用于供所述认证服务器为所述终端设备生成用户 ID。

10 以上描述了入网管理装置的内部功能和结构，如图 8b 所示，实际中，该入网管理装置可实现为电子设备，包括：存储器 84 以及处理器 85。

存储器 84，可被配置为存储其它各种数据以支持在电子设备上的操作。这些数据的示例包括用于在电子设备上操作的任何应用程序或方法的指令，联系人数据，电话簿数据，消息，图片，视频等。

15 存储器 84 可以由任何类型的易失性或非易失性存储设备或者它们的组合实现，如静态随机存取存储器（SRAM），电可擦除可编程只读存储器（EEPROM），可擦除可编程只读存储器（EPROM），可编程只读存储器（PROM），只读存储器（ROM），磁存储器，快闪存储器，磁盘或光盘。

处理器 85 与存储器 84 耦合，用于执行存储器 84 中的程序，以用于：

20 根据终端设备的入网指令，获取所述终端设备的设备 ID 以及由所述设备 ID 加密得到的用户名，所述设备 ID 是认证服务器为所述终端设备生成的；

利用与所述认证服务器约定的种子密钥对所述设备 ID 和当前时间步长内的时间值进行加密，以获得动态密码；

25 将所述用户名和所述动态密码提供给所述终端设备，以供所述终端设备生成入网认证请求并发往所述认证服务器进行入网认证。

其中，处理器 85 在执行存储器 84 中的程序时，除了上面的功能之外，还可实现其它功能，具体可参见前面各实施例中与入网管理客户端相关的描述。

进一步，如图 8b 所示，电子设备还包括：通信组件 86、显示器 87、电源组件 88、音频组件 89 等其它组件。图 8b 中仅示意性给出部分组件，并不意味着电子设备只包括
30 图 8b 所示组件。

相应地，本申请实施例还提供一种存储有计算机程序的计算机可读存储介质，所述计算机程序被计算机执行时能够实现上述各实施例中与入网管理客户端相关的方法步骤或功能。

5 图 9a 为本申请又一实施例提供的入网认证装置的结构示意图。该入网认证装置可位于需要入网认证的终端设备的内部实现。如图 9a 所示，所述入网认证装置包括：发送模块 91、获取模块 92 和生成模块 93。

发送模块 91，用于响应于入网触发操作，向入网管理客户端发送入网指令，以指示所述入网管理客户端为本端的终端设备提供入网所需的用户名和动态密码。

10 获取模块 92，用于获取所述入网管理客户端提供的所述用户名和所述动态密码；所述用户名由所述终端设备的设备 ID 加密得到，所述动态密码由所述设备 ID 和当前时间步长内的时间值加密得到，所述设备 ID 是认证服务器为所述终端设备生成的。

生成模块 93，用于根据所述用户名和所述动态密码，生成入网认证请求。

所述发送模块 91，还用于将所述入网认证请求发送给所述认证服务器，以供所述认
15 证服务器对所述终端设备进行入网认证。

在一可选实施方式中，入网认证装置还包括：显示模块，用于在响应入网触发操作时，展示入网信息页面，以获取入网认证所需的用户名和动态密码。基于此，获取模块 92 具体用于：从所述入网信息页面中获取所述用户名和所述动态密码；其中，所述用户名和所述动态密码是由所述入网管理客户端填充至所述入网信息页面中，或者由所述用
20 户从所述入网管理客户端的页面中复制到所述入网信息页面中。

以上描述了入网认证装置的内部功能和结构，如图 9b 所示，实际中，该入网认证装置可实现为终端设备，包括：存储器 95、处理器 96 以及通信组件 97。

存储器 95，可被配置为存储其它各种数据以支持在终端设备上的操作。这些数据的示例包括用于在终端设备上操作的任何应用程序或方法的指令，联系人数据，电话簿数
25 据，消息，图片，视频等。

存储器 95 可以由任何类型的易失性或非易失性存储设备或者它们的组合实现，如静态随机存取存储器（SRAM），电可擦除可编程只读存储器（EEPROM），可擦除可编程只读存储器（EPROM），可编程只读存储器（PROM），只读存储器（ROM），磁存储器，快闪存储器，磁盘或光盘。

30 处理器 96 与存储器 95 耦合，用于执行存储器 95 中的程序，以用于：

响应于入网触发操作，控制通信组件 97 向入网管理客户端发送入网指令，以指示所述入网管理客户端为所述终端设备提供入网所需的用户名和动态密码；

获取所述入网管理客户端提供的所述用户名和所述动态密码；所述用户名由所述终端设备的设备 ID 加密得到，所述动态密码由所述设备 ID 和当前时间步长内的时间值加密得到，所述设备 ID 是认证服务器为所述终端设备生成的；

根据所述用户名和所述动态密码，生成入网认证请求，并控制通信组件 97 将所述入网认证请求发送给所述认证服务器，以供所述认证服务器对所述终端设备进行入网认证。

通信组件，用于向所述入网管理客户端发送所述入网指令，并将所述入网认证请求发送给所述认证服务器。

其中，处理器 96 在执行存储器 95 中的程序时，除了上面功能之外，还可实现其它功能，具体可参见前面各实施例中与终端设备相关的描述。

进一步，如图 9b 所示，终端设备还包括：显示器 98、电源组件 99、音频组件 90 等其它组件。图 9b 中仅示意性给出部分组件，并不意味着终端设备只包括图 9b 所示组件。

相应地，本申请实施例还提供一种存储有计算机程序的计算机可读存储介质，所述计算机程序被计算机执行时能够实现上述各实施例中与终端设备相关的方法步骤或功能。

图 10a 为本申请又一实施例提供的入网认证装置的结构示意图。该入网认证装置可位于认证服务器内部实现。如图 10a 所示，所述入网认证装置包括：接收模块 1001、解密模块 1002 和验证模块 1003。

接收模块 1001，用于接收终端设备发送的入网认证请求，所述入网认证请求包括用户名和动态密码；

解密模块 1002，用于按照设定的解密算法，对所述用户名进行解密。

验证模块 1003，用于根据解密模块 1002 从用户名中解密出的所述终端设备的设备 ID 时，对所述终端设备进行可信性验证。

验证模块 1003，还用于根据可信性验证结果、所述设备 ID 和所述入网认证请求中的动态密码，对所述终端设备进行合法性验证。

在一可选实施方式中，验证模块 1003 对所述终端设备进行可信性验证时，具体用于：当从用户名中成功解密出终端设备的设备 ID 时，根据所述设备 ID 查找注册设备列表，所述注册设备列表存储有已注册设备的设备 ID；若从所述注册设备列表中查询到所述设

备 ID，查询设备状态列表，所述设备状态列表存储有已注册设备的状态；若从所述设备状态列表中查询到所述终端设备处于正常状态，确定所述终端设备通过可信性验证。

在一可选实施方式中，验证模块 1003 还用于：根据所述用户 ID 和预先注册的所述终端设备对应的用户信息，对所述终端设备所属的用户进行身份验证；当所述终端设备所属的用户通过身份验证时，执行根据所述设备 ID 对所述终端设备进行可信性验证的操作。

在一可选实施方式中，验证模块 1003 对所述终端设备进行合法性验证时，具体用于：当终端设备通过可信性验证时，利用与入网管理客户端约定的种子密钥分别对所述设备 ID 和至少两个时间步长中每个时间步长内的时间值进行加密，以生成至少两个动态密码；根据所述至少两个动态密码和所述入网认证请求中的动态密码，对所述终端设备进行合法性验证；其中，所述至少两个时间步长包括当前时间步长以及与当前时间步长相距最近的至少一个历史时间步长。

在一可选实施方式中，验证模块 1003 还用于：根据所述设备 ID 判断已认证设备的映射数据中是否存在所述终端设备上上次认证通过所使用的动态密码；若判断结果为存在，根据所述终端设备上上次认证通过所使用的动态密码和所述入网认证请求中的动态密码，对所述终端设备进行合法性验证；若判断结果为不存在，执行利用与入网管理客户端约定的种子密钥分别对所述设备 ID 和至少两个时间步长中每个时间步长内的时间值进行加密，以生成至少两个动态密码的操作。

在一可选实施方式中，入网认证装置还包括：生成模块、加密模块和发送模块。

接收模块 1001，还用于接收入网管理客户端发送的注册请求，所述注册请求携带有所述终端设备的硬件信息。

生成模块，用于根据所述硬件信息为所述终端设备生成所述设备 ID。

加密模块，用于对所述设备 ID 进行加密，生成所述用户名，并利用所述用户名和所述设备 ID 对种子密钥进行加密，以获得加密后的种子密钥。

发送模块，用于将所述用户名、所述设备 ID 以及所述加密后的种子密钥发送给所述入网管理客户端。

以上描述了入网认证装置的内部功能和结构，如图 10b 所示，实际中，该入网认证装置可实现为认证服务器，包括：存储器 1004、处理器 1005 以及通信组件 1006。

存储器 1004，可被配置为存储其它各种数据以支持在认证服务器上的操作。这些数据的示例包括用于在认证服务器上操作的任何应用程序或方法的指令，联系人数据，电

话簿数据，消息，图片，视频等。

存储器 1004 可以由任何类型的易失性或非易失性存储设备或者它们的组合实现，如静态随机存取存储器（SRAM），电可擦除可编程只读存储器（EEPROM），可擦除可编程只读存储器（EPROM），可编程只读存储器（PROM），只读存储器（ROM），磁
5 存储器，快闪存储器，磁盘或光盘。

通信组件 1006，用于接收终端设备发送的入网认证请求，所述入网认证请求包括用户名和动态密码。

处理器 1005 与存储器 1004 耦合，用于执行存储器 1004 中的程序，以用于：

按照设定的解密算法，对所述用户名进行解密；

10 根据从所述用户名中解密出的所述终端设备的设备 ID，对所述终端设备进行可信性验证；

根据可信性验证结果、所述设备 ID 和所述入网认证请求中的动态密码，对所述终端设备进行合法性验证。

其中，处理器 1005 在执行存储器 1004 中的程序时，除了上面功能之外，还可实现
15 其它功能，具体可参见前面各实施例中与认证服务器相关的描述。

进一步，如图 10b 所示，认证服务器还包括：显示器 1007、电源组件 1008、音频组件 1009 等其它组件。图 10b 中仅示意性给出部分组件，并不意味着认证服务器只包括图 10b 所示组件。

相应地，本申请实施例还提供一种存储有计算机程序的计算机可读存储介质，所述
20 计算机程序被计算机执行时能够实现上述各实施例中与认证服务器相关的方法步骤或功能。

在图 8b、图 9b 和图 10b 中的通信组件，可被配置为便于通信组件所属设备和其他设备之间有线或无线方式的通信。通信组件所属设备可以接入基于通信标准的无线网络，
25 如 WiFi，2G 或 3G，或它们的组合。在一个示例性实施例中，通信组件经由广播信道接收来自外部广播管理系统的广播信号或广播相关信息。在一个示例性实施例中，所述通信组件还包括近场通信（NFC）模块，以促进短程通信。例如，在 NFC 模块可基于射频识别（RFID）技术，红外数据协会（IrDA）技术，超宽带（UWB）技术，蓝牙（BT）技术和其他技术来实现。

30 在图 8b、图 9b 和图 10b 中的显示器，可以包括屏幕，其屏幕可以包括液晶显示器

(LCD) 和触摸面板 (TP)。如果屏幕包括触摸面板, 屏幕可以被实现为触摸屏, 以接收来自用户的输入信号。触摸面板包括一个或多个触摸传感器以感测触摸、滑动和触摸面板上的手势。所述触摸传感器可以不仅感测触摸或滑动动作的边界, 而且还检测与所述触摸或滑动操作相关的持续时间和压力。

5 在图 8b、图 9b 和图 10b 中的电源组件, 为电源组件所属设备的各种组件提供电力。电源组件可以包括电源管理系统, 一个或多个电源, 及其他与为电源组件所属设备生成、管理和分配电力相关联的组件。

10 在图 8b、图 9b 和图 10b 中的音频组件, 被配置为输出和/或输入音频信号。例如, 音频组件包括一个麦克风 (MIC), 当音频组件所属设备处于操作模式, 如呼叫模式、记录模式和语音识别模式时, 麦克风被配置为接收外部音频信号。所接收的音频信号可以被进一步存储在存储器或经由通信组件发送。在一些实施例中, 音频组件还包括一个扬声器, 用于输出音频信号。

15 本领域内的技术人员应明白, 本发明的实施例可提供为方法、系统、或计算机程序产品。因此, 本发明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, 本发明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。

20 本发明是参照根据本发明实施例的方法、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。

25 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。

30 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。

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，并不排除在包括所述要素的过程、方法、商品或者设备中还存在另外的相同要素。

以上所述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。

权 利 要 求 书

1.一种入网认证方法，其特征在于，包括：

根据终端设备的入网指令，获取所述终端设备的设备 ID 以及由所述设备 ID 加密得到的用户名，所述设备 ID 是认证服务器为所述终端设备生成的；

5 利用与所述认证服务器约定的种子密钥对所述设备 ID 和当前时间步长内的时间值进行加密，以获得动态密码；

将所述用户名和所述动态密码提供给所述终端设备，以供所述终端设备生成入网认证请求并发往所述认证服务器进行入网认证。

2.根据权利要求 1 所述的方法，其特征在于，所述将所述用户名和所述动态密码提
10 供给所述终端设备，包括：

将所述用户名和所述动态密码填充至所述终端设备提供的入网信息页面中；或者

将所述用户名和所述动态密码输出至本端页面上，并根据用户的访问请求，向所述用户展示所述本端页面，以供所述用户从所述本端页面中将所述用户名和所述动态密码复制到所述终端设备提供的入网信息页面中。

3.根据权利要求 1 或 2 所述的方法，其特征在于，所述种子密钥由独立的加密工具维护管理；

所述利用与所述认证服务器约定的种子密钥对所述设备 ID 和当前时间步长内的时间值进行加密，以获得动态密码，包括：

20 将所述设备 ID 和当前时间步长内的时间值发送给所述加密工具，以使所述加密工具利用所述种子密钥对所述设备 ID 和当前时间步长内的时间值进行加密并输出所述动态密码。

4.根据权利要求 3 所述的方法，其特征在于，在根据终端设备的入网指令，获取所述终端设备的设备 ID 以及由所述设备 ID 加密得到的用户名之前，所述方法还包括：

25 向所述认证服务器发送注册请求，所述注册请求包括所述终端设备的硬件信息，所述硬件信息用于供所述认证服务器为所述终端设备生成所述设备 ID；

接收所述认证服务器下发的所述用户名、所述设备 ID 以及由所述用户名和所述设备 ID 加密后的种子密钥；

将所述设备 ID 以及所述用户名存储在本地空间中，并将由所述用户名和所述设备 ID 加密后的种子密钥发送至所述加密工具，以供所述加密工具解密出所述种子密钥。

30 5.根据权利要求 4 所述的方法，其特征在于，所述注册请求还包括：所述终端设备

对应的用户信息；所述用户信息用于供所述认证服务器为所述终端设备生成用户 ID。

6.一种入网认证方法，其特征在于，包括：

响应于入网触发操作，向入网管理客户端发送入网指令，以指示所述入网管理客户端为本端的终端设备提供入网所需的用户名和动态密码；

5 获取所述入网管理客户端提供的所述用户名和所述动态密码；所述用户名由所述终端设备的设备 ID 加密得到，所述动态密码由所述设备 ID 和当前时间步长内的时间值加密得到，所述设备 ID 是认证服务器为所述终端设备生成的；

根据所述用户名和所述动态密码，生成入网认证请求，并将所述入网认证请求发送给所述认证服务器，以供所述认证服务器对所述终端设备进行入网认证。

10 7.根据权利要求 6 所述的方法，其特征在于，还包括：

在响应于所述入网触发操作时，展示一入网信息页面，以获取所述用户名和所述动态密码；

所述获取所述入网管理客户端提供的所述用户名和所述动态密码，包括：

从所述入网信息页面中获取所述用户名和所述动态密码；

15 其中，所述用户名和所述动态密码是由所述入网管理客户端填充至所述入网信息页面中，或者由所述用户从所述入网管理客户端的页面中复制到所述入网信息页面中。

8.一种入网认证方法，其特征在于，包括：

接收终端设备发送的入网认证请求，所述入网认证请求包括用户名和动态密码；

按照设定的解密算法，对所述用户名进行解密；

20 根据从所述用户名中解密出的所述终端设备的设备 ID，对所述终端设备进行可信性验证；

根据可信性验证结果、所述设备 ID 和所述入网认证请求中的动态密码，对所述终端设备进行合法性验证。

25 9.根据权利要求 8 所述的方法，其特征在于，所述根据从所述用户名中解密出的所述终端设备的设备 ID，对所述终端设备进行可信性验证，包括：

当从所述用户名中成功解密出所述设备 ID 时，根据所述设备 ID 查找注册设备列表，所述注册设备列表存储有已注册设备的设备 ID；

若从所述注册设备列表中查询到所述设备 ID，查询设备状态列表，所述设备状态列表存储有已注册设备的状态；

30 若从所述设备状态列表中查询到所述终端设备处于正常状态，确定所述终端设备通

过可信性验证。

10.根据权利要求 8 所述的方法，其特征在于，所述用户名中还包括：所述终端设备对应的用户 ID；

在根据从所述用户名中解密出的所述终端设备的设备 ID，对所述终端设备进行可信性验证之前，所述方法还包括：

根据所述用户 ID 和预先注册的所述终端设备对应的用户信息，对所述终端设备所属的用户进行身份验证；

当所述终端设备所属的用户通过身份验证时，执行根据所述设备 ID 对所述终端设备进行可信性验证的操作。

10 11.根据权利要求 8 所述的方法，其特征在于，所述根据可信性验证结果、所述设备 ID 和所述入网认证请求中的动态密码，对所述终端设备进行合法性验证，包括：

当所述终端设备通过可信性验证时，利用与入网管理客户端约定的种子密钥分别对所述设备 ID 和至少两个时间步长中每个时间步长内的时间值进行加密，以生成至少两个动态密码；

15 根据所述至少两个动态密码和所述入网认证请求中的动态密码，对所述终端设备进行合法性验证；

其中，所述至少两个时间步长包括当前时间步长以及与当前时间步长相距最近的至少一个历史时间步长。

20 12.根据权利要求 11 所述的方法，其特征在于，在利用与入网管理客户端约定的种子密钥分别对所述设备 ID 和至少两个时间步长中每个时间步长内的时间值进行加密，以获得至少两个动态密码之前，所述方法还包括：

根据所述设备 ID 判断已认证设备的映射数据中是否存在所述终端设备上上次认证通过所使用的动态密码；

25 若判断结果为存在，根据所述终端设备上上次认证通过所使用的动态密码和所述入网认证请求中的动态密码，对所述终端设备进行合法性验证；

若判断结果为不存在，执行利用与入网管理客户端约定的种子密钥分别对所述设备 ID 和至少两个时间步长中每个时间步长内的时间值进行加密，以生成至少两个动态密码的操作。

30 13.根据权利要求 8 所述的方法，其特征在于，在接收终端设备发送的入网认证请求之前，所述方法还包括：

接收入网管理客户端发送的注册请求，所述注册请求携带有所述终端设备的硬件信息；

根据所述硬件信息为所述终端设备生成所述设备 ID；

对所述设备 ID 进行加密，生成所述用户名；

- 5 利用所述用户名和所述设备 ID 对种子密钥进行加密，以获得加密后的种子密钥；
将所述用户名、所述设备 ID 以及所述加密后的种子密钥发送给所述入网管理客户端。

14.一种电子设备，其特征在于，包括：存储器以及处理器；

所述存储器，用于存储程序；

- 10 所述处理器，与所述存储器耦合，用于执行所述存储器中的所述程序，以用于：
根据终端设备的入网指令，获取所述终端设备的设备 ID 以及由所述设备 ID 加密得到的用户名，所述设备 ID 是认证服务器为所述终端设备生成的；

利用与所述认证服务器约定的种子密钥对所述设备 ID 和当前时间步长内的时间值进行加密，以获得动态密码；

- 15 将所述用户名和所述动态密码提供给所述终端设备，以供所述终端设备生成入网认证请求并发往所述认证服务器进行入网认证。

15.一种终端设备，其特征在于，包括：存储器、处理器以及通信组件；

所述存储器，用于存储程序；

所述处理器，与所述存储器耦合，用于执行所述存储器中的所述程序，以用于：

- 20 响应于入网触发操作，控制所述通信组件向入网管理客户端发送入网指令，以指示所述入网管理客户端为所述终端设备提供入网所需的用户名和动态密码；

获取所述入网管理客户端提供的所述用户名和所述动态密码；所述用户名由所述终端设备的设备 ID 加密得到，所述动态密码由所述设备 ID 和当前时间步长内的时间值加密得到，所述设备 ID 是认证服务器为所述终端设备生成的；

- 25 根据所述用户名和所述动态密码，生成入网认证请求，并控制所述通信组件将所述入网认证请求发送给所述认证服务器，以供所述认证服务器对所述终端设备进行入网认证；

所述通信组件，用于向所述入网管理客户端发送所述入网指令，并将所述入网认证请求发送给所述认证服务器。

- 30 16.一种认证服务器，其特征在于，存储器、通信组件以及处理器；

所述存储器，用于存储程序；

所述通信组件，用于接收终端设备发送的入网认证请求，所述入网认证请求包括用户名和动态密码；

所述处理器，与所述存储器耦合，用于执行所述存储器中的所述程序，以用于：

5 按照设定的解密算法，对所述用户名进行解密；

根据从所述用户名中解密出所述终端设备的设备 ID，对所述终端设备进行可信性验证；

根据可信性验证结果、所述设备 ID 和所述入网认证请求中的动态密码，对所述终端设备进行合法性验证。

10 17.一种认证系统，其特征在于，包括：终端设备、入网管理客户端以及认证服务器；

所述终端设备，用于响应于入网触发操作，向所述入网管理客户端发送入网指令；获取所述入网管理客户端提供的用户名和动态密码；以及根据所述用户名和所述动态密码，生成入网认证请求，并将所述入网认证请求发送给所述认证服务器；

所述入网管理客户端，用于根据所述入网指令，获取所述设备 ID 以及所述用户名；
15 利用与所述认证服务器约定的种子密钥对所述设备 ID 和当前时间步长内的时间值进行加密，以获得所述动态密码；以及将所述用户名和所述动态密码提供给所述终端设备；所述用户名由所述设备 ID 加密得到的；

所述认证服务器，用于接收所述入网认证请求，所述入网认证请求包括所述用户名和所述动态密码；根据从所述用户名中解密出的所述设备 ID，对所述终端设备进行可信性验证；以及根据可信性验证结果、所述设备 ID 和所述动态密码，对所述终端设备进行合法性验证。
20

18.根据权利要求 17 所述的系统，其特征在于，所述入网管理客户端安装于所述终端设备上。

19.根据权利要求 17 或 18 所述的系统，其特征在于，还包括：NAS 设备和 Radius
25 服务器；所述终端设备通过所述 NAS 设备与所述 Radius 服务器连接，所述 Radius 服务器与所述认证服务器连接。

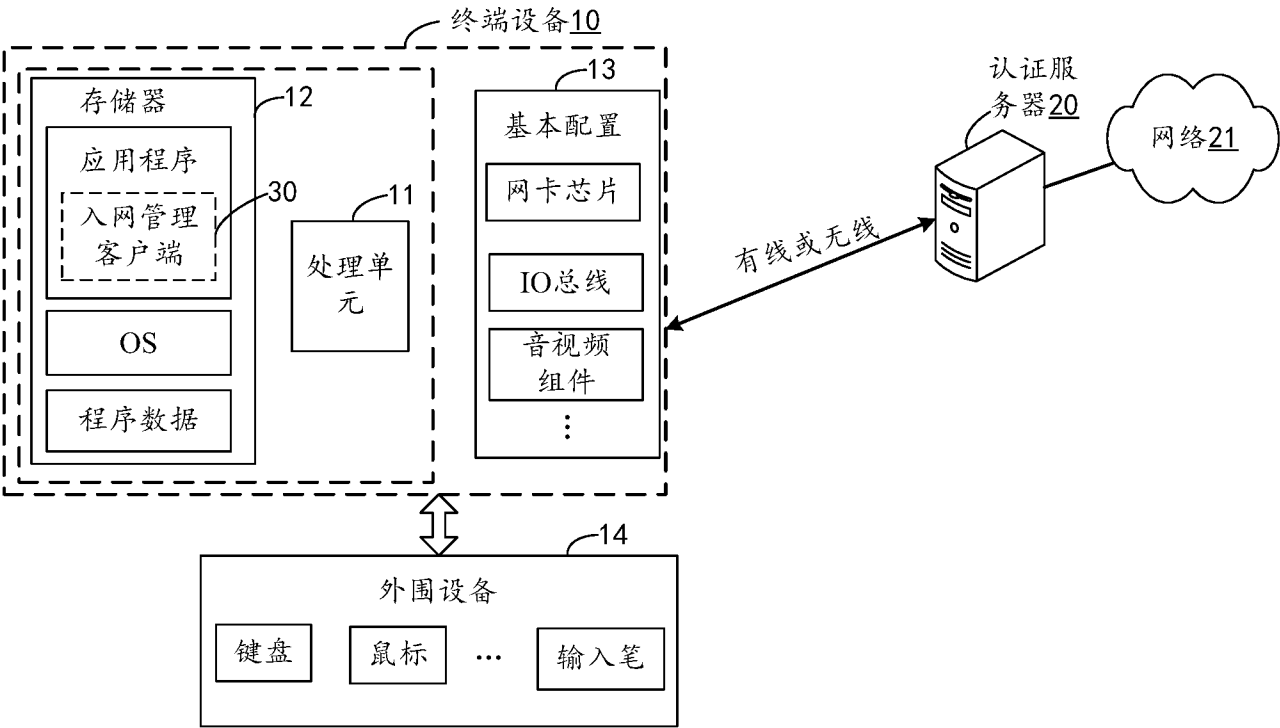


图 1

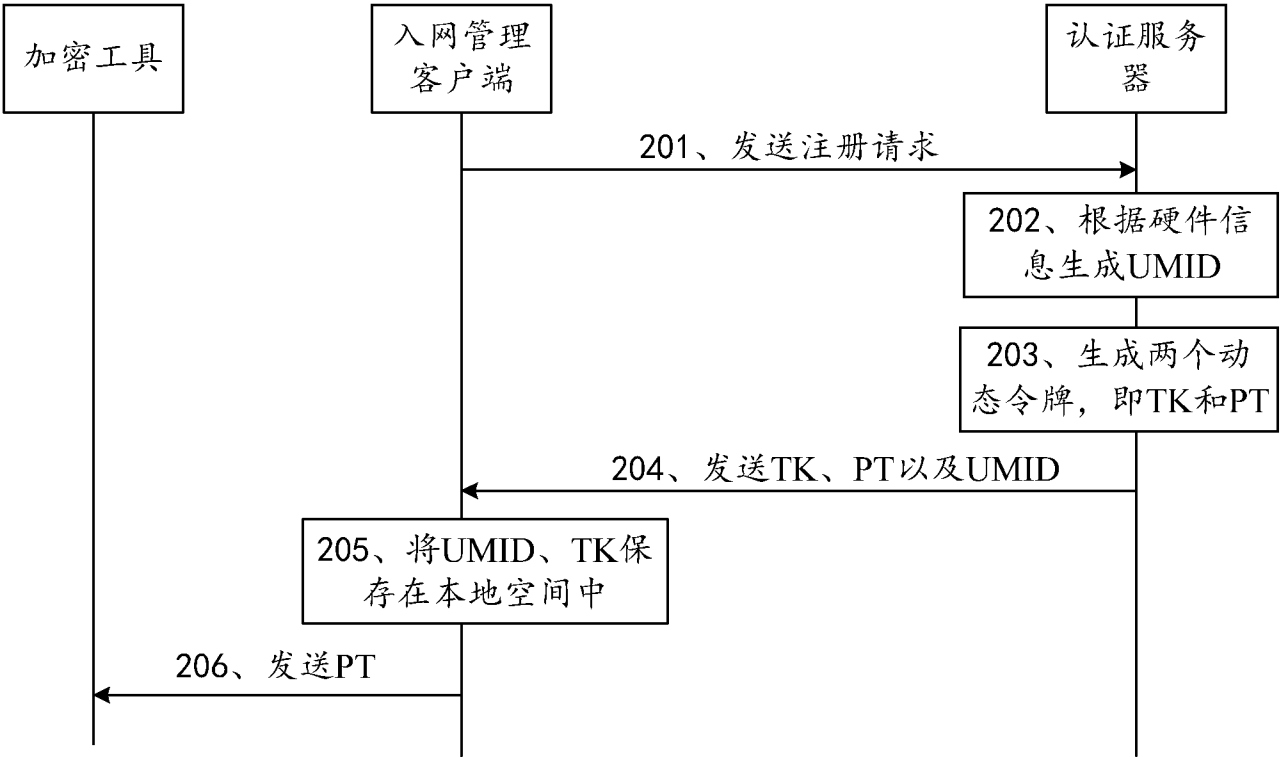


图 2

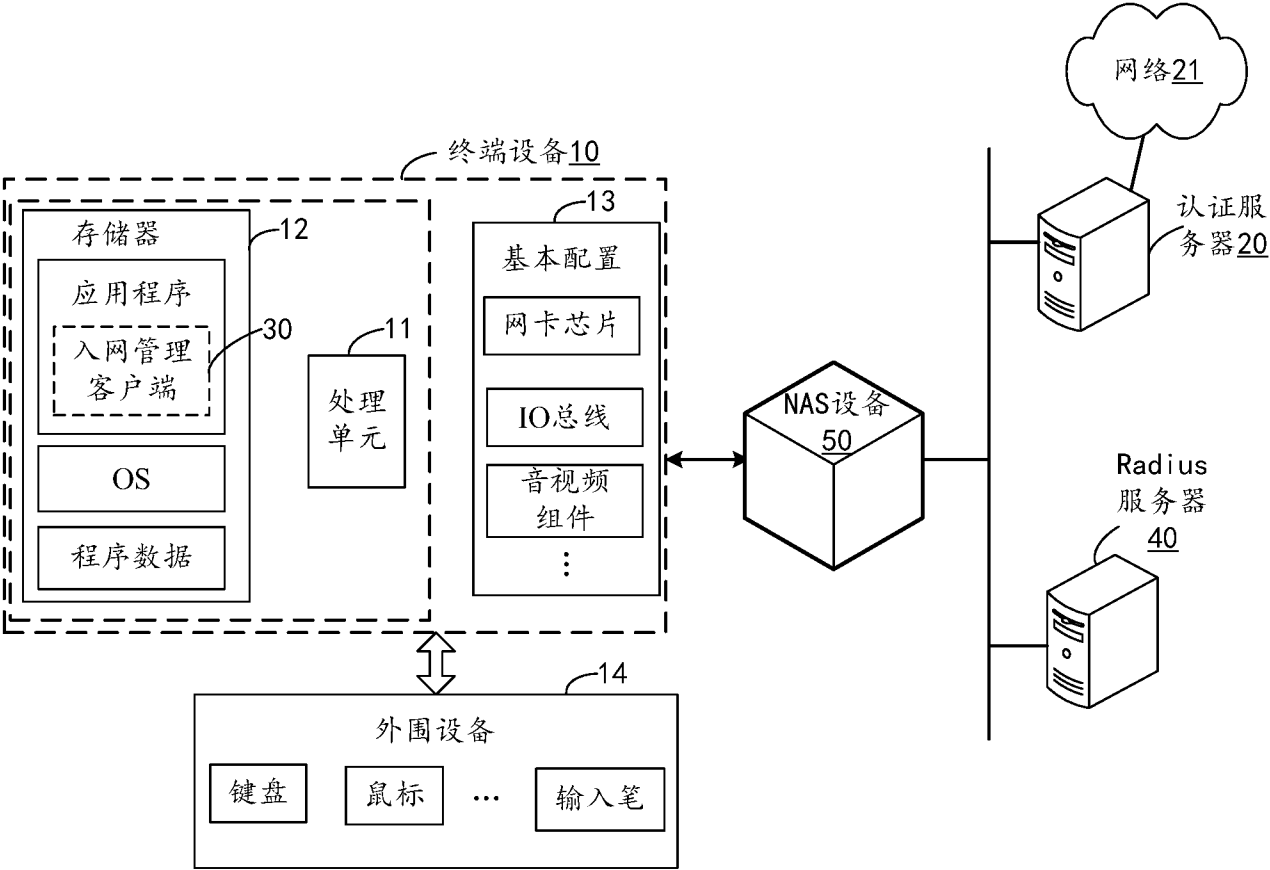


图 3

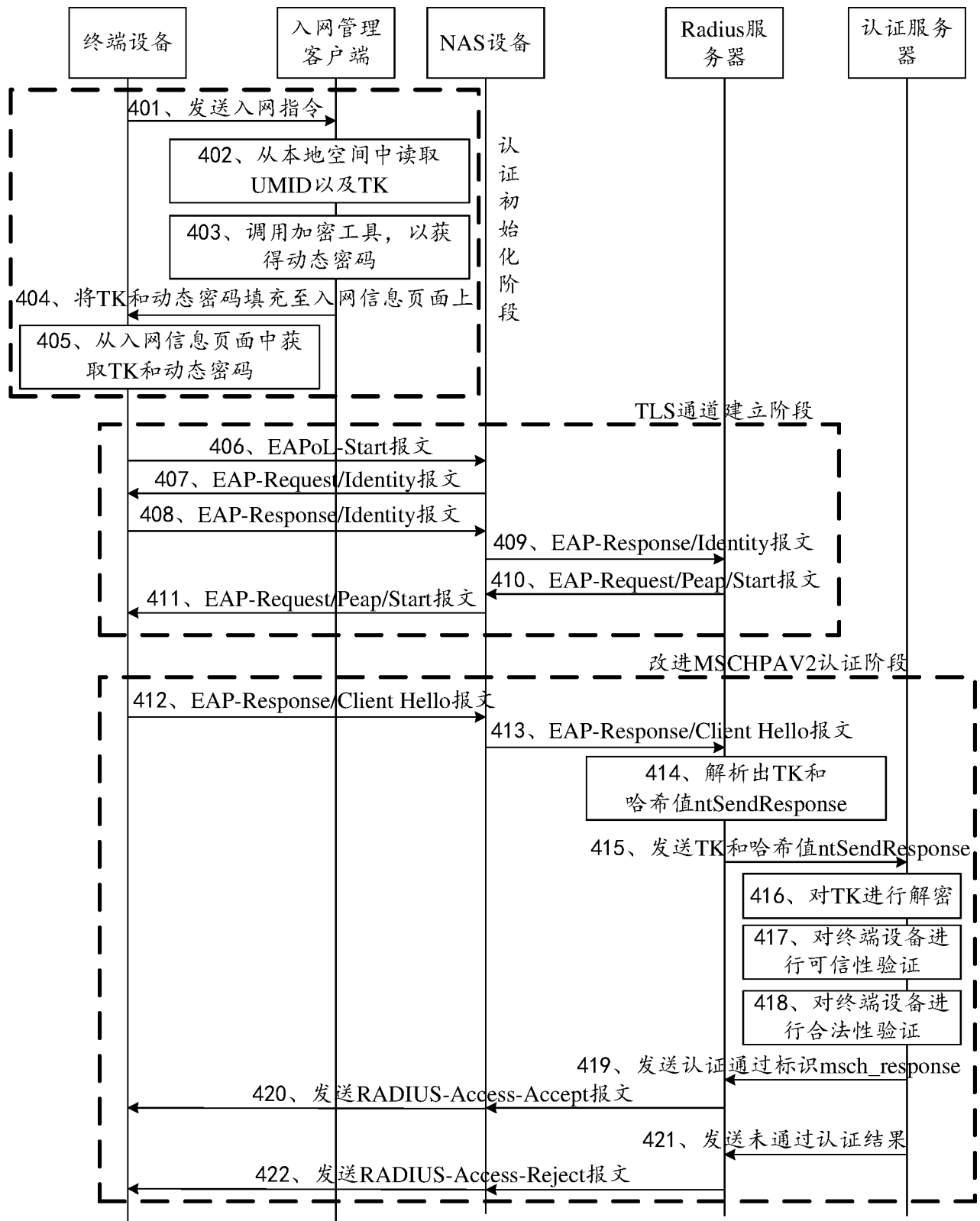


图 4

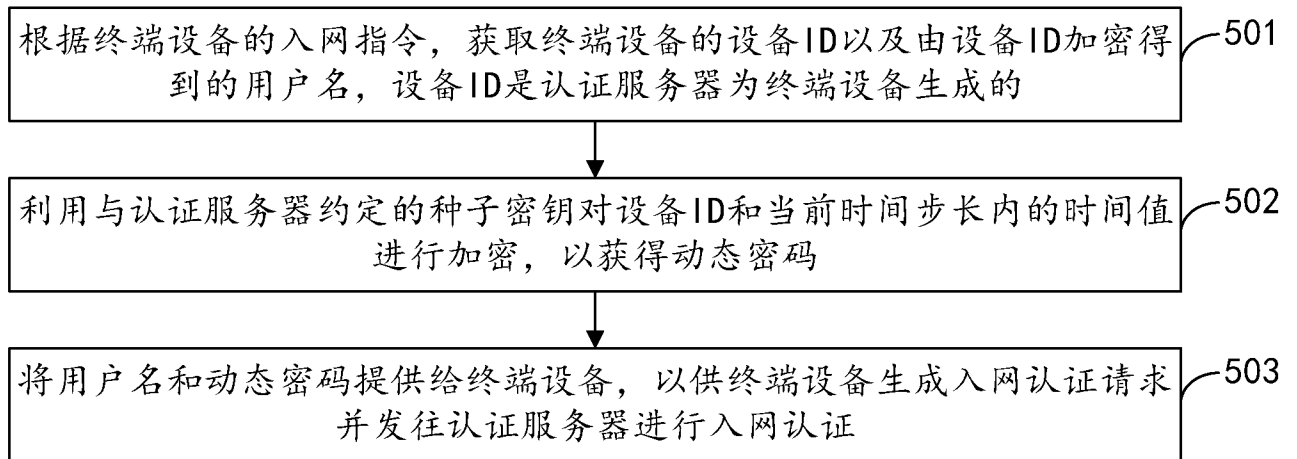


图 5

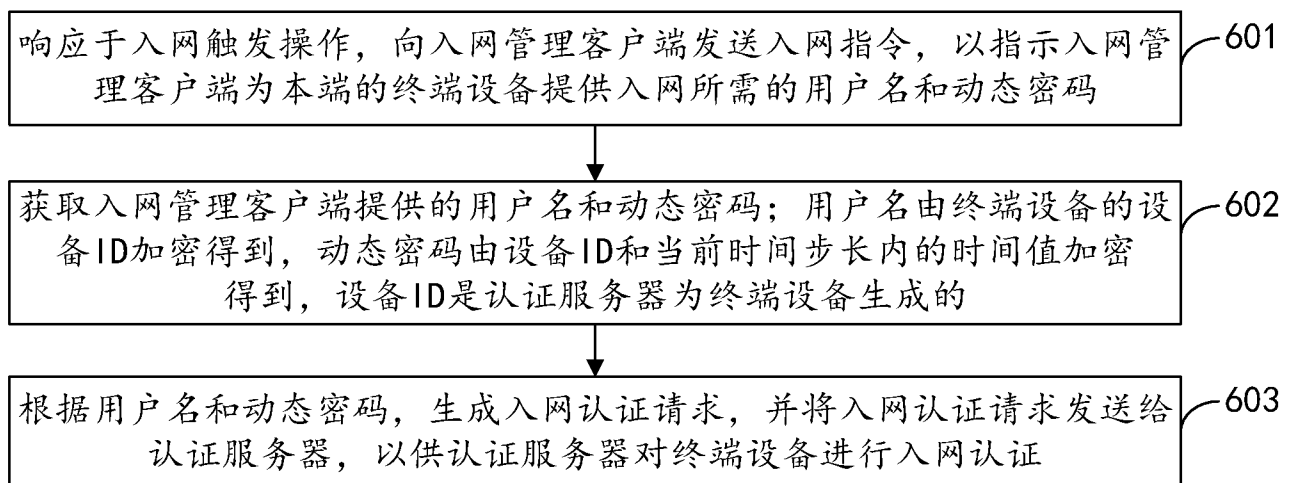


图 6

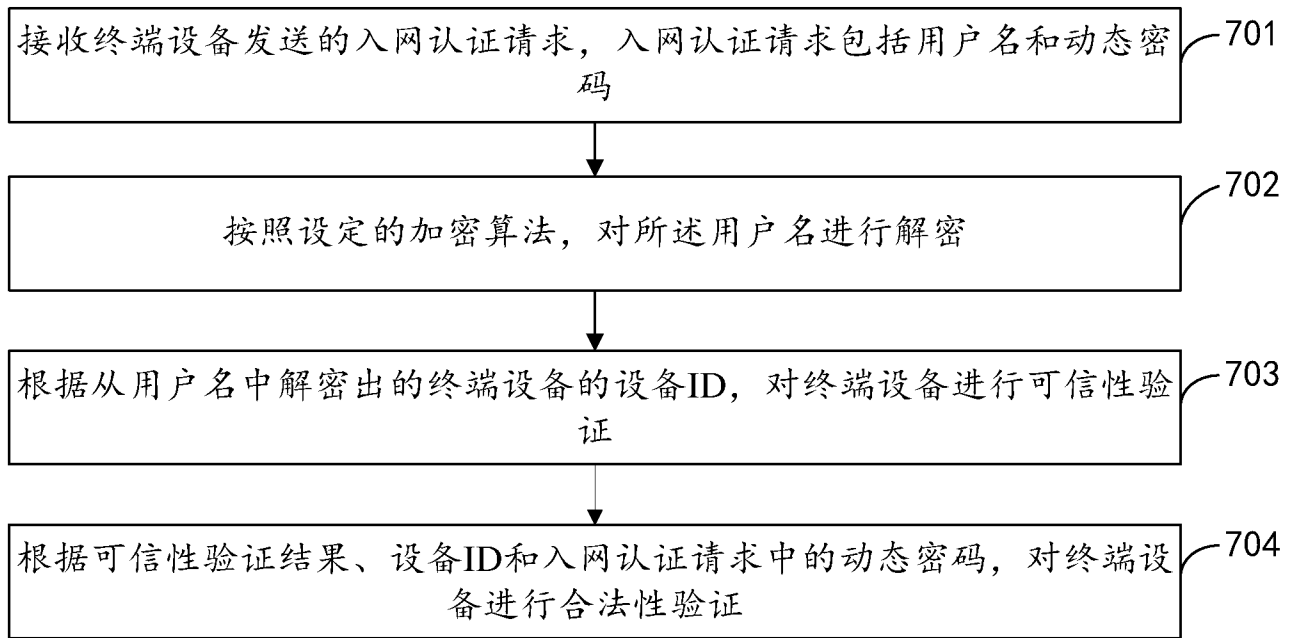


图 7

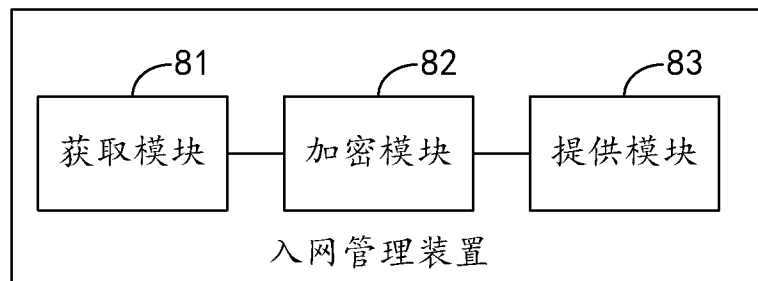


图 8a

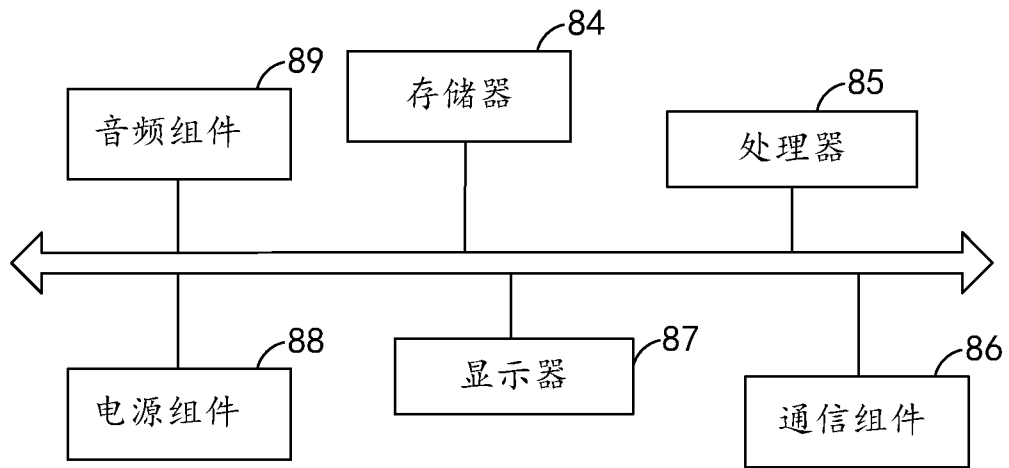


图 8b

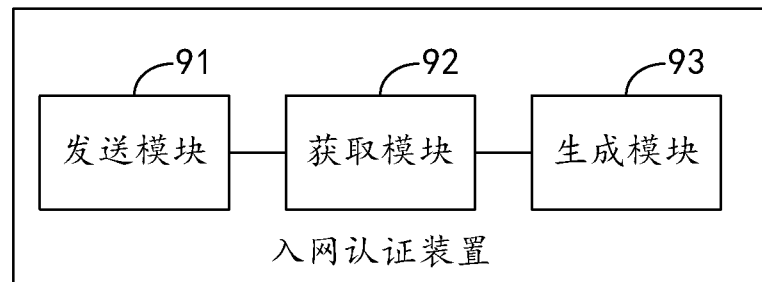


图 9a

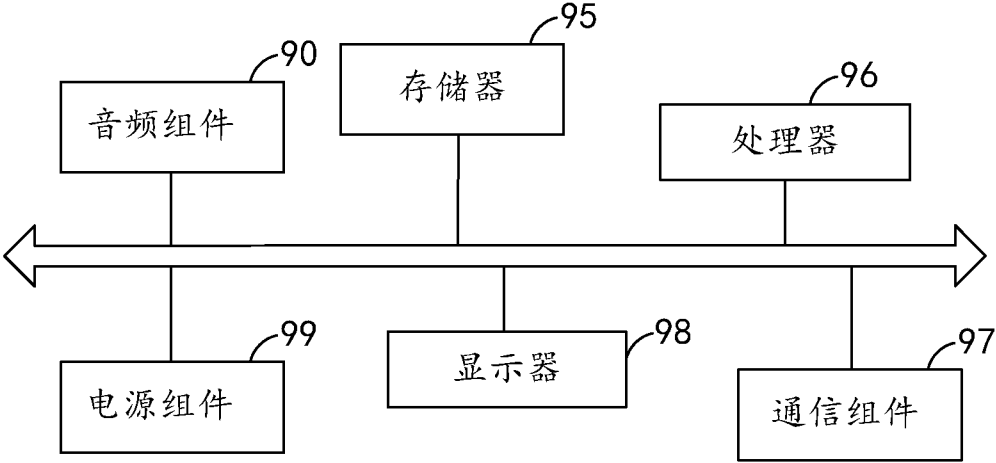


图 9b

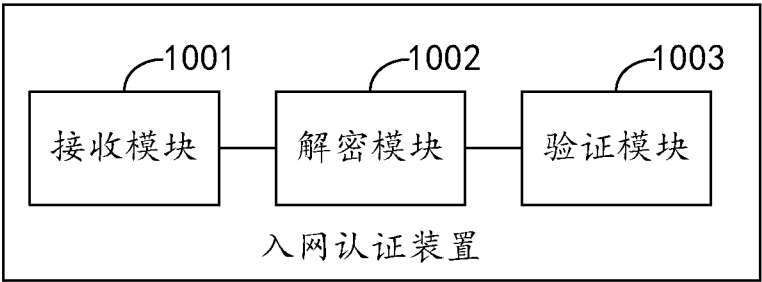


图 10a

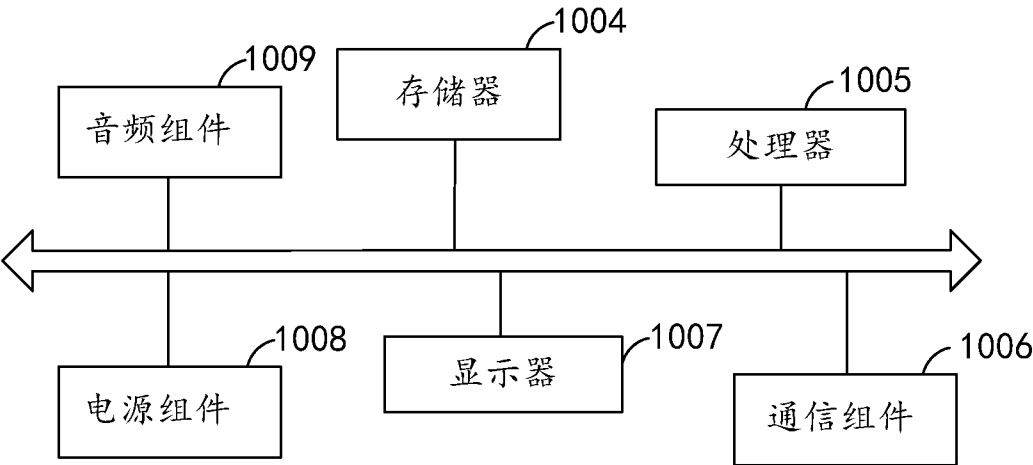


图 10b

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2018/094933

A. CLASSIFICATION OF SUBJECT MATTER

H04W 12/06(2009.01)i; H04W 12/08(2009.01)n; H04W 84/12(2009.01)n

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04W

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNABS; CNTXT; CNKI; VEN; USTXT; EPTXT; WOTXT: 接入, 认证, 热点, 无线局域网, 设备, 标识, 密码, 动态, 账号, 验证, 鉴权, access, authentication, hot spot, WLAN, WIFI, equipment, device, marking, identification, code, password

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 102378175 A (HUAWEI DEVICE CO., LTD.) 14 March 2012 (2012-03-14) description, paragraphs [0033]-[0049]	1-19
A	CN 1694555 A (BEIJING E-CHANNELS CENTURY TECHNOLOGY CO., LTD.) 09 November 2005 (2005-11-09) description page 5, paragraph 20 to page 6, paragraph 9	1-19
A	CN 104539785 A (NANJING SUPER INFORMATION TECHNOLOGY CO., LTD.) 22 April 2015 (2015-04-22) entire document	1-19

☐ Further documents are listed in the continuation of Box C.☒ See patent family annex.

* Special categories of cited documents:

“A” document defining the general state of the art which is not considered to be of particular relevance

“E” earlier application or patent but published on or after the international filing date

“L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

“O” document referring to an oral disclosure, use, exhibition or other means

“P” document published prior to the international filing date but later than the priority date claimed

“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

“&” document member of the same patent family

Date of the actual completion of the international search

03 September 2018

Date of mailing of the international search report

25 September 2018

Name and mailing address of the ISA/CN

State Intellectual Property Office of the P. R. China
No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing
100088
China

Facsimile No. (86-10)62019451

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2018/094933

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	102378175	A	14 March 2012	KR	20140066241	A	30 May 2014
				US	2014215583	A1	31 July 2014
				EP	2753108	A2	09 July 2014
				KR	101642203	B1	22 July 2016
				WO	2012136163	A3	29 November 2012
				WO	2012136163	A2	11 October 2012
				AU	2012239202	A1	24 April 2014
				US	9462468	B2	04 October 2016
				JP	2014534674	A	18 December 2014
				JP	5897137	B2	30 March 2016
				EP	2753108	A4	21 January 2015
CN	1694555	A	09 November 2005	CN	100518411	C	22 July 2009
CN	104539785	A	22 April 2015	CN	104539785	B	01 February 2017

国际检索报告

国际申请号

PCT/CN2018/094933

A. 主题的分类

H04W 12/06(2009.01)i; H04W 12/08(2009.01)n; H04W 84/12(2009.01)n

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

H04W

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称, 和使用的检索词(如使用))

CNABS;CNTXT;CNKI;VEN;USTXT;EPTXT;WOTXT: 接入, 认证, 热点, 无线局域网, 设备, 标识, 密码, 动态, 账号, 验证, 鉴权, access, authentication, hot spot, WLAN, WIFI, equipment, device, marking, identification, code, password

C. 相关文件

类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求
A	CN 102378175 A (华为终端有限公司) 2012年 3月 14日 (2012 - 03 - 14) 说明书第[0033]段-第[0049]段	1-19
A	CN 1694555 A (北京易诚世纪科技有限公司) 2005年 11月 9日 (2005 - 11 - 09) 说明书第5页第20段-第6页第9段	1-19
A	CN 104539785 A (南京速帕信息科技有限公司) 2015年 4月 22日 (2015 - 04 - 22) 全文	1-19

☐ 其余文件在C栏的续页中列出。☒ 见同族专利附件。

* 引用文件的具体类型:

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件 (如具体说明的)

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期

2018年 9月 3日

国际检索报告邮寄日期

2018年 9月 25日

ISA/CN的名称和邮寄地址

中华人民共和国国家知识产权局(ISA/CN)
中国北京市海淀区蓟门桥西土城路6号 100088

受权官员

陈晓霞

传真号 (86-10) 62019451

电话号码 (86-512) 88996090

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2018/094933

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	102378175	A	2012年 3月 14日	KR	20140066241	A	2014年 5月 30日
				US	2014215583	A1	2014年 7月 31日
				EP	2753108	A2	2014年 7月 9日
				KR	101642203	B1	2016年 7月 22日
				WO	2012136163	A3	2012年 11月 29日
				WO	2012136163	A2	2012年 10月 11日
				AU	2012239202	A1	2014年 4月 24日
				US	9462468	B2	2016年 10月 4日
				JP	2014534674	A	2014年 12月 18日
				JP	5897137	B2	2016年 3月 30日
				EP	2753108	A4	2015年 1月 21日
CN	1694555	A	2005年 11月 9日	CN	100518411	C	2009年 7月 22日
CN	104539785	A	2015年 4月 22日	CN	104539785	B	2017年 2月 1日

表 PCT/ISA/210 (同族专利附件) (2015年1月)