(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 118139047 A
(43)申请公布日 2024.06.04

(21)申请号 202211503692.2

(22)申请日 2022.11.28

(71)申请人 大唐移动通信设备有限公司
地址 100085 北京市海淀区上地东路5号院1号楼1层

(72)发明人 梁亚从 王胡成 陈山枝

(74)专利代理机构 北京银龙知识产权代理有限公司 11243
专利代理师 王丹

(51)Int.Cl.
H04W 12/069(2021.01)
H04W 4/06(2009.01)
H04L 9/32(2006.01)

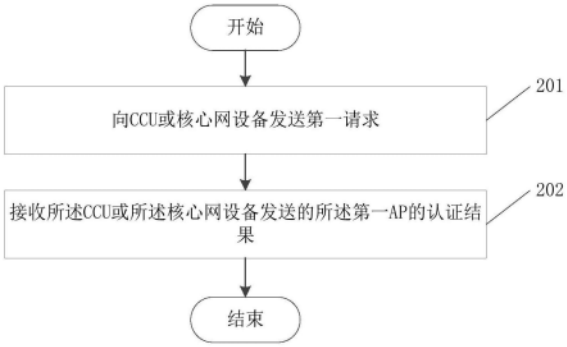
权利要求书3页 说明书20页 附图11页

(54)发明名称

一种接入点认证方法、装置及可读存储介质

(57)摘要

本申请公开了一种接入点认证方法、装置及可读存储介质，涉及通信技术领域，以降低网络时延。该方法包括：向CCU或核心网设备发送第一请求，所述第一请求用于请求所述CCU或者所述核心网设备对第一AP进行认证；接收所述CCU或所述核心网设备发送的所述第一AP的认证结果；本申请实施例可降低网络时延。



CN 118139047 A

1.一种接入点认证方法,应用于终端,其特征在于,包括:

向云化控制单元CCU或核心网设备发送第一请求,所述第一请求用于请求所述CCU或者所述核心网设备对第一接入点AP进行认证;

接收所述CCU或所述核心网设备发送的所述第一AP的认证结果;

其中,所述认证结果是由所述CCU或所述核心网设备根据从认证信息存储设备获取的第一认证信息对所述第一AP进行认证得到的。

2.根据权利要求1所述的接入点认证方法,其特征在于,所述向云化控制单元CCU或核心网设备发送第一请求,包括:

通过第二AP向所述CCU或所述核心网设备发送所述第一请求,所述第一请求携带第二认证信息,所述第二认证信息包括所述第一AP的第二数字证书;或者

通过第二AP向所述CCU发送测量上报消息,所述第一请求包括所述测量上报消息;

其中,所述第二AP为已认证的AP。

3.根据权利要求2所述的接入点认证方法,其特征在于,所述方法还包括:

从所述第一AP获取所述第二数字证书。

4.一种接入点认证方法,应用于CCU或核心网设备,其特征在于,包括:

获取第一AP的第二认证信息;

从认证信息存储设备获取所述第一AP的第一认证信息;

根据所述第二认证信息和所述第一认证信息对所述第一AP进行认证,得到认证结果;

向终端发送所述认证结果。

5.根据权利要求4所述的接入点认证方法,其特征在于,所述第二认证信息包括第二数字证书或第二数字证书哈希值;

所述获取第一AP的第二认证信息,包括:

接收所述终端通过第二AP发送的第一请求,所述第一请求携带所述第二认证信息,所述第二认证信息包括所述第一AP的第二数字证书;或者

接收所述终端通过第二AP发送的测量上报消息;根据所述测量上报消息从所述第一AP获取所述第一AP的第二数字证书;或者

接收所述终端通过第二AP发送的所述第一请求,所述第一请求携带所述第二认证信息,所述第二认证信息包括所述第一AP的第二数字证书;确定所述第二数字证书的第二数字证书哈希值;

其中,所述第二AP为已认证的AP。

6.根据权利要求4所述的接入点认证方法,其特征在于,所述第一认证信息包括第一数字证书或第一数字证书哈希值;

所述从认证信息存储设备获取所述第一AP的第一认证信息,包括:

从所述认证信息存储设备获取所述第一AP的第一数字证书;或者

从所述认证信息存储设备获取所述第一AP的第一数字证书哈希值。

7.根据权利要求4所述的接入点认证方法,其特征在于,所述第二认证信息包括所述第一AP的第二数字证书,所述第一认证信息包括所述第一AP的第一数字证书;

所述根据所述第二认证信息和所述第一认证信息对所述第一AP进行认证,得到认证结果,包括:

将所述第一数字证书和所述第二数字证书进行比较,得到所述认证结果。

8.根据权利要求4所述的接入点认证方法,其特征在于,所述第二认证信息包括所述第一AP的第二数字证书哈希值,所述第一认证信息包括所述第一AP的第一数字证书哈希值;

所述根据所述第二认证信息和所述第一认证信息对所述第一AP进行认证,得到认证结果,包括:

将所述第一数字证书哈希值和所述第二数字证书哈希值进行比较,得到所述认证结果。

9.根据权利要求6所述的接入点认证方法,其特征在于,所述方法还包括:

向所述认证信息存储设备存储所述CCU或所述核心网设备对应的域内的AP的数字证书和/或数字证书哈希值。

10.根据权利要求4至9任一项所述的方法,其特征在于,所述认证信息存储设备包括区块链。

11.一种接入点认证方法,应用于第一AP,其特征在于,包括:

向终端发送第二请求,所述第二请求用于表示所述第一AP为待认证的AP;

向所述终端或CCU发送第二认证信息,所述第二认证信息用于通过所述终端发送给所述CCU或核心网设备,或者直接发送给所述CCU,并由所述CCU或所述核心网设备根据从认证信息存储设备获取的第一认证信息对所述第一AP进行认证。

12.根据权利要求11所述的接入点认证方法,其特征在于,向CCU发送第二认证信息,包括:

接收所述CCU的第三请求;

响应于所述第三请求,向所述CCU发送所述第二认证信息;所述第二认证信息包括所述第一AP的第二数字证书。

13.一种接入点认证装置,应用于终端,其特征在于,包括:存储器,收发机,处理器:

存储器,用于存储计算机程序;收发机,用于在所述处理器的控制下收发数据;处理器,用于读取所述存储器中的计算机程序并执行以下操作:

向CCU或核心网设备发送第一请求,所述第一请求用于请求所述CCU或者所述核心网设备对第一接入点AP进行认证;

接收所述CCU或所述核心网设备发送的所述第一AP的认证结果;

其中,所述认证结果是由所述CCU或所述核心网设备根据从认证信息存储设备获取的第一认证信息对所述第一AP进行认证得到的。

14.一种接入点认证装置,应用于CCU或核心网设备,其特征在于,包括:存储器,收发机,处理器:

存储器,用于存储计算机程序;收发机,用于在所述处理器的控制下收发数据;处理器,用于读取所述存储器中的计算机程序并执行以下操作:

获取第一AP的第二认证信息;

从认证信息存储设备获取所述第一AP的第一认证信息;

根据所述第二认证信息和所述第一认证信息对所述第一AP进行认证,得到认证结果;

向终端发送所述认证结果。

15.一种接入点认证装置,应用于第一AP,其特征在于,包括:存储器,收发机,处理器:

向终端发送第二请求,所述第二请求用于表示所述第一AP为待认证的AP;

向所述终端或CCU发送第二认证信息,所述第二认证信息用于通过所述终端发送给所述CCU或核心网设备,或者直接发送给所述CCU,并由所述CCU或所述核心网设备根据从认证信息存储设备获取的第一认证信息对所述第一AP进行认证。

16.一种接入点认证装置,应用于终端,其特征在于,包括:

第一发送单元,用于向CCU或核心网设备发送第一请求,所述第一请求用于请求所述CCU或者所述核心网设备对第一接入点AP进行认证;

第一接收单元,用于接收所述CCU或所述核心网设备发送的所述第一AP的认证结果;

其中,所述认证结果是由所述CCU或所述核心网设备根据从认证信息存储设备获取的第一认证信息对所述第一AP进行认证得到的。

17.一种接入点认证装置,应用于CCU或核心网设备,其特征在于,包括:

第一获取单元,用于获取第一AP的第二认证信息;

第二获取单元,用于从认证信息存储设备获取所述第一AP的第一认证信息;

第一认证单元,用于根据所述第二认证信息和所述第一认证信息对所述第一AP进行认证,得到认证结果;

第一发送单元,用于向终端发送所述认证结果。

18.一种接入点认证装置,应用于第一AP,其特征在于,包括:

第一发送单元,用于向终端发送第二请求,所述第二请求用于表示所述第一AP为待认证的AP;

第二发送单元,用于向所述终端或CCU发送第二认证信息,所述第二认证信息用于通过所述终端发送给所述CCU或核心网设备,或者直接发送给所述CCU,并由所述CCU或所述核心网设备根据从认证信息存储设备获取的第一认证信息对所述第一AP进行认证。

19.一种处理器可读存储介质,其特征在于,所述处理器可读存储介质存储有计算机程序,所述计算机程序用于使所述处理器执行权利要求1至12任一项所述的接入点认证方法。

一种接入点认证方法、装置及可读存储介质

技术领域

[0001] 本申请涉及通信技术领域,尤其涉及一种接入点(Access point,接入点)认证方法、装置及可读存储介质。

背景技术

[0002] 在UCMN(User-Centric Mobile Network,以用户为中心的移动网络)网络架构下,接入点的覆盖范围小,功能多样化,数量众多,未来将向即插即用的方向发展。由于AP的部署方式灵活多样,因此导致管理AP的难度增大,存在不可控的安全威胁较高。为此,需要对AP进行认证。

[0003] 目前,在对AP进行认证时采用的是双重双向鉴权的方式。但是,由于AP数量众多,这种方式的信令流程交互较多,从而导致网络时延增加。

发明内容

[0004] 本申请实施例提供一种接入点认证方法、装置及可读存储介质,以降低网络时延。

[0005] 第一方面,本申请实施例提供了一种接入点认证方法,应用于终端,包括:

[0006] 向CCU(Cloud-based Control Unit,云化控制单元)或核心网设备发送第一请求,所述第一请求用于请求所述CCU或者所述核心网设备对第一AP(Access Point,接入点)进行认证;

[0007] 接收所述CCU或所述核心网设备发送的所述第一AP的认证结果;

[0008] 其中,所述认证结果是由所述CCU或所述核心网设备根据从认证信息存储设备获取的第一认证信息对所述第一AP进行认证得到的。

[0009] 可选的,所述向云化控制单元CCU或核心网设备发送第一请求,包括:

[0010] 通过第二AP向所述CCU或所述核心网设备发送所述第一请求,所述第一请求携带第二认证信息,所述第二认证信息包括所述第一AP的第二数字证1书;或者

[0011] 通过第二AP向所述CCU发送测量上报消息,所述第一请求包括所述测量上报消息;

[0012] 其中,所述第二AP为已认证的AP。

[0013] 可选的,所述方法还包括:

[0014] 从所述第一AP获取所述第二数字证书。

[0015] 第二方面,本申请实施例提供了一种接入点认证方法,应用于CCU或核心网设备,包括:

[0016] 获取第一AP的第二认证信息;

[0017] 从认证信息存储设备获取所述第一AP的第一认证信息;

[0018] 根据所述第二认证信息和所述第一认证信息对所述第一AP进行认证,得到认证结果;

[0019] 向终端发送所述认证结果。

[0020] 可选的,所述第二认证信息包括第二数字证书或第二数字证书哈希值;

[0021] 所述获取第一AP的第二认证信息,包括:

[0022] 接收所述终端通过第二AP发送的第一请求,所述第一请求携带所述第二认证信息,所述第二认证信息包括所述第一AP的第二数字证书;或者

[0023] 接收所述终端通过第二AP发送的测量上报消息;根据所述测量上报消息从所述第一AP获取所述第一AP的第二数字证书;或者

[0024] 接收所述终端通过第二AP发送的所述第一请求,所述第一请求携带所述第二认证信息,所述第二认证信息包括所述第一AP的第二数字证书;确定所述第二数字证书的第二数字证书哈希值;

[0025] 其中,所述第二AP为已认证的AP。

[0026] 可选的,所述第一认证信息包括第一数字证书或第一数字证书哈希值;

[0027] 所述从认证信息存储设备获取所述第一AP的第一认证信息,包括:

[0028] 从所述认证信息存储设备获取所述第一AP的第一数字证书;或者

[0029] 从所述认证信息存储设备获取所述第一AP的第一数字证书哈希值。

[0030] 可选的,所述第二认证信息包括所述第一AP的第二数字证书,所述第一认证信息包括所述第一AP的第一数字证书;

[0031] 所述根据所述第二认证信息和所述第一认证信息对所述第一AP进行认证,得到认证结果,包括:

[0032] 将所述第一数字证书和所述第二数字证书进行比较,得到所述认证结果。

[0033] 可选的,所述第二认证信息包括所述第一AP的第二数字证书哈希值,所述第一认证信息包括所述第一AP的第一数字证书哈希值;

[0034] 所述根据所述第二认证信息和所述第一认证信息对所述第一AP进行认证,得到认证结果,包括:

[0035] 将所述第一数字证书哈希值和所述第二数字证书哈希值进行比较,得到所述认证结果。

[0036] 可选的,所述方法还包括:

[0037] 向所述认证信息存储设备存储所述CCU或所述核心网设备对应的域内的AP的数字证书和/或数字证书哈希值。

[0038] 可选的,所述认证信息存储设备包括区块链。

[0039] 第三方面,本申请实施例提供了一种接入点认证方法,应用于第一AP,包括:

[0040] 向终端发送第二请求,所述第二请求用于表示所述第一AP为待认证的AP;

[0041] 向所述终端或CCU发送第二认证信息,所述第二认证信息用于通过所述终端发送给所述CCU或核心网设备,或者直接发送给所述CCU,并由所述CCU或所述核心网设备根据从认证信息存储设备获取的第一认证信息对所述第一AP进行认证。

[0042] 可选的,向CCU发送第二认证信息,包括:

[0043] 接收所述CCU的第三请求;

[0044] 响应于所述第三请求,向所述CCU发送所述第二认证信息;所述第二认证信息包括所述第一AP的第二数字证书。

[0045] 第四方面,本申请实施例提供了一种接入点认证装置,应用于终端,包括:存储器,收发机,处理器:

[0046] 存储器,用于存储计算机程序;收发机,用于在所述处理器的控制下收发数据;处理器,用于读取所述存储器中的计算机程序并执行以下操作:

[0047] 向CCU或核心网设备发送第一请求,所述第一请求用于请求所述CCU或者所述核心网设备对第一接入点AP进行认证;

[0048] 接收所述CCU或所述核心网设备发送的所述第一AP的认证结果;

[0049] 其中,所述认证结果是由所述CCU或所述核心网设备根据从认证信息存储设备获取的第一认证信息对所述第一AP进行认证得到的。

[0050] 第五方面,本申请实施例提供了一种接入点认证装置,应用于CCU或核心网设备,包括:存储器,收发机,处理器:

[0051] 存储器,用于存储计算机程序;收发机,用于在所述处理器的控制下收发数据;处理器,用于读取所述存储器中的计算机程序并执行以下操作:

[0052] 获取第一AP的第二认证信息;

[0053] 从认证信息存储设备获取所述第一AP的第一认证信息;

[0054] 根据所述第二认证信息和所述第一认证信息对所述第一AP进行认证,得到认证结果;

[0055] 向终端发送所述认证结果。

[0056] 第六方面,本申请实施例提供了一种接入点认证装置,应用于第一AP,包括:存储器,收发机,处理器:

[0057] 向终端发送第二请求,所述第二请求用于表示所述第一AP为待认证的AP;

[0058] 向所述终端或CCU发送第二认证信息,所述第二认证信息用于通过所述终端发送给所述CCU或核心网设备,或者直接发送给所述CCU,并由所述CCU或所述核心网设备根据从认证信息存储设备获取的第一认证信息对所述第一AP进行认证。

[0059] 第七方面,本申请实施例提供了一种接入点认证装置,应用于终端,包括:

[0060] 第一发送单元,用于向CCU或核心网设备发送第一请求,所述第一请求用于请求所述CCU或者所述核心网设备对第一接入点AP进行认证;

[0061] 第一接收单元,用于接收所述CCU或所述核心网设备发送的所述第一AP的认证结果;

[0062] 其中,所述认证结果是由所述CCU或所述核心网设备根据从认证信息存储设备获取的第一认证信息对所述第一AP进行认证得到的。

[0063] 4第八方面,本申请实施例提供了一种接入点认证装置,应用于CCU或核心网设备,包括:

[0064] 第一获取单元,用于获取第一AP的第二认证信息;

[0065] 第二获取单元,用于从认证信息存储设备获取所述第一AP的第一认证信息;

[0066] 第一认证单元,用于根据所述第二认证信息和所述第一认证信息对所述第一AP进行认证,得到认证结果;

[0067] 第一发送单元,用于向终端发送所述认证结果。

[0068] 第九方面,本申请实施例提供了一种接入点认证装置,应用于第一AP,包括:

[0069] 第一发送单元,用于向终端发送第二请求,所述第二请求用于表示所述第一AP为待认证的AP;

[0070] 第二发送单元,用于向所述终端或CCU发送第二认证信息,所述第二认证信息用于通过所述终端发送给所述CCU或核心网设备,或者直接发送给所述CCU,并由所述CCU或所述核心网设备根据从认证信息存储设备获取的第一认证信息对所述第一AP进行认证。

[0071] 第十方面,本申请实施例还提供一种通信设备,包括:收发机、存储器、处理器及存储在存储器上并可在处理器上运行的程序,所述处理器执行所述程序时实现如上所述的接入点认证方法中的步骤。

[0072] 第十一方面,本申请实施例还提供一种处理器可读存储介质,所述可读存储介质上存储计算机程序,所述计算机程序被处理器执行时实现如上所述的接入点认证方法中的步骤。

[0073] 在本申请实施例中,利用CCU或核心网设备根据从认证信息存储设备获取的第一认证信息对所述第一AP进行认证可得到认证结果,从而简化了信令交互流程,降低了网络时延。

附图说明

[0074] 图1是UCMN网络的架构示意图;

[0075] 图2是本申请实施例提供的接入点认证方法的流程图之一;

[0076] 图3是本申请实施例提供的接入点认证方法的流程图之二;

[0077] 图4是本申请实施例提供的接入点认证方法的流程图之三;

[0078] 图5是本申请实施例提供的接入点认证方法的流程图之四;

[0079] 图6是本申请实施例的应用场景示意图之一;

[0080] 图7是本申请实施例提供的接入点认证方法的流程图之五;

[0081] 图8是本申请实施例提供的接入点认证方法的流程图之六;

[0082] 图9是本申请实施例的应用场景示意图之二;

[0083] 图10是本申请实施例的应用场景示意图之三;

[0084] 图11是本申请实施例提供的接入点认证方法的流程图之七;

[0085] 图12是本申请实施例的应用场景示意图之四;

[0086] 图13(a)是本申请实施例的应用场景示意图之五;

[0087] 图13(b)是本申请实施例提供的接入点认证方法的流程图之八;

[0088] 图14是本申请实施例提供的接入点认证装置的结构图之一;

[0089] 图15是本申请实施例提供的接入点认证装置的结构图之二;

[0090] 图16是本申请实施例提供的接入点认证装置的结构图之三;

[0091] 图17是本申请实施例提供的接入点认证装置的结构图之四;

[0092] 图18是本申请实施例提供的接入点认证装置的结构图之五;

[0093] 图19是本申请实施例提供的接入点认证装置的结构图之六;

[0094] 图20是本申请实施例提供的接入点认证装置的结构图之七;

[0095] 图21是本申请实施例提供的接入点认证装置的结构图之八。

具体实施方式

[0096] 本申请实施例中术语“和/或”,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。字符“/”一般表示前后关联对象是一种“或”的关系。

[0097] 本申请实施例中术语“多个”是指两个或两个以上,其它量词与之类似。

[0098] 下面将结合本申请实施例中的附图,对本申请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申请一部分实施例,并不是全部的实施例。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。

[0099] 本申请实施例提供了一种接入点认证方法、装置及可读存储介质,用以降低网络时延。

[0100] 其中,方法和装置是基于同一申请构思的,由于方法和装置解决问题的原理相似,因此装置和方法的实施可以相互参见,重复之处不再赘述。

[0101] 参见图1,图1是UCMN网络的架构示意图。包括:

[0102] CCU(Cloud-based Control Unit,云化控制单元):包括管理平面和控制平面。。其中,CCU功能包括:传统的控制平面功能,如AS(Access Stratum,接入层)/NAS(Non-Access Stratum,非接入层)相关的系统信息管理;寻呼控制;RRC(Radio Resource Control,无线资源控制)连接的建立、维护和释放;安全功能,包括密钥管理;承载管理;流动性管理;UE(User Equipment,用户设备)测量报告管理;NAS信息传输等。与5G CU不同的是,它不具备用户面功能。此外,CCU还执行UCMN的特定功能,如UE上下文管理、AP管理和选择等。

[0103] DDU(Distributed Data Unit,分布式数据单元):用户面锚点。现有技术中的CU(Central Unit,集中单元)-UP(User Plane,用户面)功能位于DDU中。DDU还承担了一些资源管理和AP节点选择的功能,如L1(层1)测量管理和动态资源调度。

[0104] AP:RAN(Radio Access Network,无线接入网络)接入点,直接连接到UE。

[0105] UCMN网络实现了“网络跟随用户”的理念。对于单个用户来说,它总能获得其所在位置周围的网络节点所能提供的最佳服务。其中引入了Flexible Cell(灵活小区)的概念,终端始终处于Flexible Cell的中心。终端周围关联一个或多个接入节点AP,这若干个AP共同为终端服务,其中构成Flexible Cell的AP集合根据用户的移动性、业务变化或信道变化而动态变化;调度和传输由唯一的终端标识(UE-ID)解决,与单个AP标识或小区特定的终端标识无关。

[0106] 以下,结合不同的实施例描述本申请实施例的接入点认证方法的实现过程。

[0107] 参见图2,图2是本申请实施例提供的接入点认证方法的流程图,应用于终端,如图2所示,包括以下步骤:

[0108] 步骤201、向CCU或核心网设备发送第一请求,所述第一请求用于请求所述CCU或者所述核心网设备对第一AP进行认证。

[0109] 其中,第一AP指的是待认证的AP。若第一AP请求加入其它的域中,该第一AP可向终端发送广播消息,以表示该第一AP请求加入其它的域中或表示该第一AP为待认证的AP。可选的,该广播消息中还可包括第一AP的待认证的认证信息,如数字证书等。在本申请实施例中,将第一AP的待认证的认证信息作为第二认证信息。当然,第二认证信息在本申请实施例中还可包括其他内容,例如,第一AP的数字证书的哈希值等。

[0110] 其中,所述CCU或核心网设备(例如,可以是AUSF(Authentication Server

Function,鉴权服务功能))所在的域为受终端信任的域。在本申请实施例中,CCU和核心网设备都可对AP进行认证。例如,在多个CCU连接到同一个核心网的场景中,每个域(domain)中都具有CCU,如果一个域中的AP需要加入到另一个域(受终端信任的域)中时,该另一个域中的CCU可对该AP进行认证。例如,在多个CCU连接到不同核心网的场景中,不同的核心网代表不同的域。每个域(domain)中都具有核心网设备,CCU。如果一个域中的AP需要加入到另一个域(受终端信任的域)中时,该另一个域中的核心网设备或CCU可对该AP进行认证。上述两种情形可称为跨域的认证。除了跨域认证之外,也可对同一域内的AP进行认证。此时,域中的CCU可对该AP进行认证。

[0111] 在此步骤中,终端可根据该第一AP的广播消息,通过第二AP向所述CCU或所述核心网设备发送所述第一请求,所述第一请求携带第二认证信息,所述第二认证信息包括所述第一AP的第二数字证书。其中,所述第二AP为已认证的AP。对于域内认证的场景,所述第一请求包括终端的测量上报消息。终端可通过第二AP向所述CCU发送测量上报消息,以指示需要对第一AP进行认证。

[0112] 可选的,在本申请实施例中,终端还可通过第一AP的广播消息获取第一AP的数字证书,在此,将其称为第二数字证书。

[0113] 步骤202、接收所述CCU或所述核心网设备发送的所述第一AP的认证结果;其中,所述认证结果是由所述CCU或所述核心网设备根据从认证信息存储设备获取的第一认证信息对所述第一AP进行认证得到的。

[0114] 在本申请实施例中,所述认证信息存储设备用于存储已认证的AP的认证信息,如数字证书,数字证书哈希值等,并可根据CCU或者核心网设备的请求,向CCU或核心网设备提供待认证AP的数字证书或数字证书哈希值。同时,认证信息存储设备还可保证存储的认证信息的安全性。可选的,在本申请实施例中,可采用区块链作为认证信息存储设备。从而,可利用区块链的特点,便捷的实现上述功能。

[0115] 在获得第一AP的认证结果后,若认证结果表示认证通过,则终端可接入该第一AP,否则可不接入。

[0116] 在本申请实施例中,利用CCU或核心网设备根据从认证信息存储设备获取的第一认证信息对所述第一AP进行认证可得到认证结果,从而简化了信令交互流程,降低了网络时延。

[0117] 参见图3,图3是本申请实施例提供的接入点认证方法的流程图,应用于CCU,如图3所示,包括以下步骤:

[0118] 步骤301、获取第一AP的第二认证信息。

[0119] 在本申请实施例中,所述第二认证信息包括第二数字证书或第二数字证书哈希值。哈希(Hash)算法是一种从任意文件中创造小的数字指纹的方法,很难找到两段不同的明文使得它们的hash值一致,以及将任意大的文件映射为固定长度的特性,这使得哈希算法在安全校验得到广泛应用。因此,也可被用作进行信息认证。

[0120] 若第二认证信息包括第二数字证书,那么,CCU可接收所述终端通过第二AP发送的第一请求,所述第一请求携带所述第二认证信息,所述第二认证信息包括所述第一AP的第二数字证书;或者,CCU可接收所述终端通过第二AP发送的测量上报消息,并根据所述测量上报消息从所述第一AP获取所述第一AP的第二数字证书。其中,所述第二AP为已认证的AP。

当然,CCU还可通过其他方式获取第二数字证书,以上只是举例说明了几种可能的实现方式。

[0121] 若第二认证信息包括第二数字证书哈希值,那么,CCU可接收所述终端通过第二AP发送的所述第一请求,所述第一请求携带所述第二认证信息,所述第二认证信息包括所述第一AP的第二数字证书。CCU根据获得的第二数字证书,确定所述第二数字证书的第二数字证书哈希值。也就是说,在这种方式中,CCU在获得了第二数字证书后,自行确定第二数字证书哈希值。其中,在本申请实施例中,CCU可通过多种方式获得第二数字证书哈希值,本申请实施例并不对其进行限定。

[0122] 步骤302、从认证信息存储设备获取所述第一AP的第一认证信息。

[0123] 如前所述,在本申请实施例中,所述认证信息存储设备用于存储已认证的AP的认证信息,如数字证书,数字证书哈希值等,并可根据CCU或者核心网设备的请求,向CCU或核心网设备提供待认证AP的数字证书或数字证书哈希值。同时,认证信息存储设备还需保证存储的认证信息的安全性。可选的,在本申请实施例中,可采用区块链作为认证信息存储设备。从而,可利用区块链的特点,便捷的实现上述功能。

[0124] 在此步骤中,CCU可根据第二认证信息从认证信息存储设备获取所述第一AP的第一认证信息。例如,CCU可通过代理服务器向认证信息存储设备发送第一AP的标识,以获取第一AP的第一认证信息。其中,所述第一认证信息包括第一数字证书或第一数字证书哈希值。那么,相应的,CCU可从所述认证信息存储设备获取所述第一AP的第一数字证书;或者,从所述认证信息存储设备获取所述第一AP的第一数字证书哈希值。

[0125] 步骤303、根据所述第二认证信息和所述第一认证信息对所述第一AP进行认证,得到认证结果。

[0126] 在此步骤中,CCU可将数字证书进行对比,也可将数字证书哈希值进行对比。

[0127] 如果所述第二认证信息包括所述第一AP的第二数字证书,所述第一认证信息包括所述第一AP的第一数字证书,那么,CCU可将所述第一数字证书和所述第二数字证书进行比较,得到所述认证结果。也即,在这种方式中是将数字证书进行对比。如果二者一致,那么认证结果为认证通过;否则为认证不通过。

[0128] 如果所述第二认证信息包括所述第一AP的第二数字证书哈希值,所述第一认证信息包括所述第一AP的第一数字证书哈希值,那么,CCU可将所述第一数字证书哈希值和所述第二数字证书哈希值进行比较,得到所述认证结果。也即,在这种方式中是将数字证书哈希值进行对比。如果二者一致,那么认证结果为认证通过;否则为认证不通过。

[0129] 步骤304、向终端发送所述认证结果。

[0130] 在本申请实施例中,不对CCU向终端发送认证结果的方式进行限定。例如,CCU可隐性或者显性的向终端指示或发送该认证结果。具体的,CCU可直接将该认证结果发送给终端;或者向终端发送一个指示,并通过该指示的不同取值表示该认证结果的不同内容等。

[0131] 可选的,在本申请实施例中,为提高认证效率,CCU还可将CCU所属域内的AP的数字证书和/或数字证书哈希值存储到认证信息存储设备中。通过存储数字证书哈希值的方式,可节约认证信息存储设备的存储空间,降低对其存储能力的要求。

[0132] 在本申请实施例中,利用CCU或核心网设备根据从认证信息存储设备获取的第一认证信息对所述第一AP进行认证可得到认证结果,从而简化了信令交互流程,降低了网络

时延。

[0133] 参见图4,图4是本申请实施例提供的接入点认证方法的流程图,应用于核心网设备,如图4所示,包括以下步骤:

[0134] 步骤401、获取第一AP的第二认证信息。

[0135] 在本申请实施例中,所述第二认证信息包括第二数字证书或第二数字证书哈希值。

[0136] 若第二认证信息包括第二数字证书,那么,核心网设备可接收所述终端通过第二AP发送的第一请求,所述第一请求携带所述第二认证信息,所述第二认证信息包括所述第一AP的第二数字证书。其中,所述第二AP为已认证的AP。当然,核心网设备还可通过其他方式获取第二数字证书,以上只是举例说明了几种可能的实现方式。

[0137] 若第二认证信息包括第二数字证书哈希值,那么,核心网设备可接收所述终端通过第二AP发送的所述第一请求,所述第一请求携带所述第二认证信息,所述第二认证信息包括所述第一AP的第二数字证书。核心网设备根据获得的第二数字证书,确定所述第二数字证书的第二数字证书哈希值。也就是说,在这种方式中,核心网设备在获得了第二数字证书后,自行确定第二数字证书哈希值。其中,在本申请实施例中,核心网设备可通过多种方式获得第二数字证书哈希值,本申请实施例并不对其进行限定。

[0138] 步骤402、从认证信息存储设备获取所述第一AP的第一认证信息。

[0139] 如前所述,在本申请实施例中,所述认证信息存储设备用于存储已认证的AP的认证信息,如数字证书,数字证书哈希值等,并可根据核心网设备或者核心网设备的请求,向核心网设备或核心网设备提供待认证AP的数字证书或数字证书哈希值。同时,认证信息存储设备还需保证存储的认证信息的安全性。可选的,在本申请实施例中,可采用区块链作为认证信息存储设备。从而,可利用区块链的特点,便捷的实现上述功能。

[0140] 在此步骤中,核心网设备可根据第二认证信息从认证信息存储设备获取所述第一AP的第一认证信息。例如,核心网设备可向认证信息存储设备发送第一AP的标识,以获取第一AP的第一认证信息。其中,所述第一认证信息包括第一数字证书或第一数字证书哈希值。那么,相应的,核心网设备可从所述认证信息存储设备获取所述第一AP的第一数字证书;或者,从所述认证信息存储设备获取所述第一AP的第一数字证书哈希值。

[0141] 步骤403、根据所述第二认证信息和所述第一认证信息对所述第一AP进行认证,得到认证结果。

[0142] 在此步骤中,核心网设备可将数字证书进行对比,也可将数字证书哈希值进行对比。

[0143] 如果所述第二认证信息包括所述第一AP的第二数字证书,所述第一认证信息包括所述第一AP的第一数字证书,那么,核心网设备可将所述第一数字证书和所述第二数字证书进行比较,得到所述认证结果。也即,在这种方式中是将数字证书进行对比。如果二者一致,那么认证结果为认证通过;否则为认证不通过。

[0144] 如果所述第二认证信息包括所述第一AP的第二数字证书哈希值,所述第一认证信息包括所述第一AP的第一数字证书哈希值,那么,核心网设备可将所述第一数字证书哈希值和所述第二数字证书哈希值进行比较,得到所述认证结果。也即,在这种方式中是将数字证书哈希值进行对比。如果二者一致,那么认证结果为认证通过;否则为认证不通过。

[0145] 步骤404、向终端发送所述认证结果。

[0146] 在本申请实施例中,不对核心网设备向终端发送认证结果的方式进行限定。例如,核心网设备可隐性或者显性的向终端指示或发送该认证结果。具体的,核心网设备可直接将该认证结果发送给终端;或者向终端发送一个指示,并通过该指示的不同取值表示该认证结果的不同内容等。

[0147] 可选的,在本申请实施例中,为提高认证效率,核心网设备还可将核心网设备所属域内的AP的数字证书和/或数字证书哈希值存储到认证信息存储设备中。

[0148] 在本申请实施例中,利用核心网设备或核心网设备根据从认证信息存储设备获取的第一认证信息对所述第一AP进行认证可得到认证结果,从而简化了信令交互流程,降低了网络时延。

[0149] 参见图5,图5是本申请实施例提供的接入点认证方法的流程图,应用于第一AP,如图5所示,包括以下步骤:

[0150] 步骤501、向终端发送第二请求,所述第二请求用于表示所述第一AP为待认证的AP,以请求进行认证。

[0151] 其中,所述第二请求可以通过广播消息的形式实现,同时可携带第一AP的待认证信息,如数字证书等。

[0152] 步骤502、向所述终端或CCU发送第二认证信息,所述第二认证信息用于通过所述终端发送给所述CCU或核心网设备,或者直接发送给所述CCU,并由所述CCU或所述核心网设备根据从认证信息存储设备获取的第一认证信息对所述第一AP进行认证。

[0153] 如前所述,CCU或核心网设备都可对第一AP进行认证。在不同的认证方式下,第一AP可向不同的实体发送器第二认证信息。例如,若由CCU进行认证,那么,第一AP可向终端发送第二认证信息,并由终端向CCU发送该第二认证信息,或者,第一AP还可应CCU的请求直接将第二认证信息发送给CCU。例如,第一AP接收所述CCU的第三请求,响应于所述第三请求,向所述CCU发送所述第二认证信息;所述第二认证信息包括所述第一AP的第二数字证书。

[0154] 若由核心网设备进行认证,那么,第一AP可向终端发送第二认证信息,并由终端向核心网设备发送该第二认证信息。

[0155] 在本申请实施例中,利用核心网设备或核心网设备根据从认证信息存储设备获取的第一认证信息对所述第一AP进行认证可得到认证结果,从而简化了信令交互流程,降低了网络时延。

[0156] 现有技术中的双向鉴权的方式,首先在一个APG(Access Point Group,接入点集合)中选出代表节点AP作为代表,进行终端与LSC(Location Services,位置服务)的网络双向鉴权。在终端与LSC进行网络鉴权之后,为了保证用户接入合法AP,终端与目标AP再次进行接入层双向鉴权。因此,在上述过程中,终端每次切换至不同运营商的AP都要进行一次网络层双向鉴权以及一次接入层双向鉴权,交互流程较多,降低了网络鉴权效率,拖慢了AP之间的切换速度,降低了用户体验;而且,在这个过程中,与LSC进行鉴权之后,为了确定AP的合法性,终端需再次与AP鉴权,从而消耗了终端的电量,占据了终端的大量资源。

[0157] 为此,在本申请实施例中,提出了通过CCU或者核心网设备对AP进行认证的方案。

[0158] 即插即用的AP认证场景如图6所示。由于用户(终端)的移动性,域2内的AP需要加入Flexible Cell为终端服务,因此,为了认证新加入AP的合法性,受终端信任的域1需要对

新加入的AP进行认证。其中,各个域内的CCU通过代理服务器将各自域内AP的数字证书发送至区块链上存储,基于区块链的不可篡改性以及共识机制,各AP的认证信息不会被篡改。图6所示的场景可称为跨域认证。

[0159] 参见图7,图7是本申请实施例的接入点认证方法的流程图。结合图7,该过程可包括:

[0160] 步骤701、待认证AP通过广播消息发送待认证的数字证书(即第二数字证书,图6中的数字证书1,2)。

[0161] 步骤702、由于终端的移动性,需要进行Flexible Cell的动态更新,终端通过待认证AP发送的广播消息得到待认证AP的第二数字证书,并将其发送给受信任AP。

[0162] 步骤703、受信任AP(即第二AP)将第二数字证书发送至信任域内的CCU。

[0163] 步骤704、信任域内的CCU通过区块链代理服务器从区块链获取待认证AP的第一数字证书(图6中的数字证书1',2')。

[0164] 具体的,信任域内的CCU向代理服务器申请获取待认证AP的第一数字证书,代理服务器从区块链下载该第一数字证书。之后,代理服务器将从区块链获取的第一数字证书发送给CCU。

[0165] 步骤705、信任域内的CCU执行认证过程,即通过比对待认证AP发送的第二数字证书和从区块链下载的第一数字证书,确定待认证AP是否为合法AP,得到认证结果。例如,若第二数字证书和第一数字证书一致,则确定待认证AP合法;否则不合法。

[0166] 步骤706、信任域内的CCU向终端发送该认证结果。

[0167] 之后,终端可根据该认证结果选择是否接入该待认证AP等。

[0168] 在本申请实施例中,采用哈希值上链,即各个域内的CCU通过代理服务器将各自域内AP的数字证书的哈希值发送至区块链上存储。由于区块链上存储的不是完整的数字证书而是哈希值,从而减少了对部署区块链的服务器的存储能力要求。该实施例所适用的场景仍如图6所示。不同的是,在此实施例中,CCU从区块链获取的是数字整数哈希值,认证过程也是将数字证书哈希值进行对比。

[0169] 参见图8,图8是本申请实施例的接入点认证方法的流程图。结合图8,该过程可包括:

[0170] 步骤801、待认证AP通过广播消息发送待认证的数字证书(即第二数字证书)。

[0171] 步骤802、由于终端的移动性,需要进行Flexible Cell的动态更新,终端通过待认证AP发送的广播消息得到待认证AP的第二数字证书,并将其发送给受信任AP。

[0172] 步骤803、受信任AP(即第二AP)将第二数字证书发送至信任域内的CCU。

[0173] 步骤804、信任域内的CCU通过区块链代理服务器从区块链获取待认证AP的第一数字证书哈希值。

[0174] 具体的,信任域内的CCU向代理服务器申请获取待认证AP的第一数字证书哈希值,代理服务器从区块链获取该第一数字证书哈希值。之后,代理服务器将从区块链获取的第一数字证书哈希值发送给CCU。

[0175] 步骤805、信任域内的CCU计算第二数字证书的哈希值,得到第二数字证书哈希值。

[0176] 步骤806、信任域内的CCU执行认证过程,即通过比对第二数字证书哈希值和第一数字证书哈希值,确定待认证AP是否为合法AP,得到认证结果。例如,若第二数字证书哈希

值和第一数字证书哈希值一致,则确定待认证AP合法;否则不合法。

[0177] 步骤807、信任域内的CCU向终端发送该认证结果。

[0178] 之后,终端可根据该认证结果选择是否接入该待认证AP等。

[0179] 参见图9,图9是本申请实施例的一种场景示意图。在该场景中,当Flexible Cell新加入的AP为域内AP时,需要在域内对新加入的AP进行认证。待认证的AP通过广播消息广播其数字证书,由终端通过受信任AP将其数字证书发送给CCU进行认证。具体的,这种场景下的认证过程可参照图7或图8所示的实施例的认证过程。

[0180] 参见图10,图10是本申请实施例的一种场景示意图。在这种场景下,终端通过测量上报消息向CCU提供待认证AP的信息,由于该待认证AP可接入域内CCU中,因此,CCU可通知待认证AP发送数字证书至CCU进行认证。参见图11,图11是本申请实施例的接入点认证方法的流程图。结合图11,该过程可包括:

[0181] 步骤1101、待认证AP向终端发送广播消息,可表示该AP为待认证的AP。

[0182] 步骤1102、终端通过待认证AP发送的广播消息得到待认证AP的信息,如标识等。终端向受信任AP(即第二AP)发送测量上报消息。

[0183] 步骤1103、受信任AP(即第二AP)转发测量上报消息。

[0184] 步骤1104、信任域内的CCU通过区块链代理服务器从区块链获取待认证AP的第一数字证书。

[0185] 具体的,信任域内的CCU向代理服务器申请获取待认证AP的第一数字证书,代理服务器从区块链下载该第一数字证书。之后,代理服务器将从区块链获取的第一数字证书发送给CCU。

[0186] 步骤1105、信任域内的CCU向待认证AP发送请求,请求其提供第二数字证书。

[0187] 步骤1106、待认证AP向信任域内的CCU提供第二数字证书。

[0188] 步骤1107、信任域内的CCU执行认证过程,即通过比对第二数字证书和第一数字证书,确定待认证AP是否为合法AP,得到认证结果。例如,若第二数字证书和第一数字证书一致,则确定待认证AP合法;否则不合法。

[0189] 步骤1108、信任域内的CCU向终端发送该认证结果。

[0190] 之后,终端可根据该认证结果选择是否接入该待认证AP等。

[0191] 本申请实施例的另一场景中,涉及两个核心网,需要进行跨网对AP进行认证。不同的核心网代表不同域。在这种场景中,可采用CCU或者核心网设备进行认证。

[0192] 其中,图12为采用CCU进行认证的过程示意图。CCU将域内的AP的数字证书上链。在对待认证AP进行认证时,通过将从终端收到的待认证AP的数字证书和从区块链网络上下载的数字证书进行对比进行认证。其具体流程可参照前述图7或图8所示实施例的描述。

[0193] 其中,图13(a)为采用核心网进行认证的过程示意图。AP认证跨越不同核心网,认证工作在核心网设备进行。核心网设备将域内的AP的数字证书上链,通过将从终端收到的待认证AP的数字证书和从区块链网络上下载的数字证书进行对比进行认证。。参见图13(b),具体过程可包括:

[0194] 步骤1301、待认证AP通过广播消息发送待认证的数字证书(即第二数字证书)。

[0195] 步骤1302、由于终端的移动性,需要进行Flexible Cell的动态更新,终端通过待认证AP发送的广播消息得到待认证AP的第二数字证书,并将其发送给受信任AP。

[0196] 步骤1303、受信任AP(即第二AP)将第二数字证书发送至信任域内的CCU。

[0197] 步骤1304、信任域内的CCU将第二数字证书至核心网设备。

[0198] 步骤1305、核心网设备通过区块链代理服务器从区块链获取待认证AP的第一数字证书。

[0199] 步骤1306、核心网设备执行认证过程,即通过比对待认证AP发送的第二数字证书和从区块链下载的第一数字证书,确定待认证AP是否为合法AP,得到认证结果。例如,若第二数字证书和第一数字证书一致,则确定待认证AP合法;否则不合法。

[0200] 步骤1307、核心网设备通过信任域内的CCU向终端发送该认证结果。

[0201] 之后,终端可根据该认证结果选择是否接入该待认证AP等。

[0202] 在此实施例中,核心网设备在获得了第二数字证书之后,步骤1305可替代的为从区块链网络获得第一数字证书哈希值。同时,核心网设备计算第二数字证书的第二数字证书哈希值。在认证的过程中,核心网设备可将所述第一数字证书哈希值和所述第二数字证书哈希值进行比较,得到所述认证结果。也即,在这种方式中是将数字证书哈希值进行对比。如果二者一致,那么认证结果为认证通过;否则为认证不通过。

[0203] 在本申请实施例中,利用CCU或核心网设备根据从区块链获取的认证信息对待认证AP进行认证可得到认证结果,从而简化了信令交互流程,降低了网络时延。同时,利用区块链存储AP的数字证书,CCU或核心网设备能够随时访问区块链网络获取AP的数字证书,能够解决对AP的跨域认证问题。

[0204] 本申请实施例提供的技术方案可以适用于多种系统,尤其是5G系统。例如适用的系统可以是全球移动通讯(global system of mobile communication,GSM)系统、码分多址(code division multiple access,CDMA)系统、宽带码分多址(Wideband Code Division Multiple Access,WCDMA)通用分组无线业务(general packet radio service,GPRS)系统、长期演进(long term evolution,LTE)系统、LTE频分双工(frequency division duplex,FDD)系统、LTE时分双工(time division duplex,TDD)系统、高级长期演进(long term evolution advanced,LTE-A)系统、通用移动系统(universal mobile telecommunication system,UMTS)、全球互联微波接入(worldwide interoperability for microwave access,WiMAX)系统、5G新空口(New Radio,NR)系统等。这多种系统中均包括终端设备和网络设备。系统中还可以包括核心网部分,例如演进的分组系统(Evolved Packet System,EPS)、5G系统(5GS)等。

[0205] 本申请实施例涉及的终端设备,可以是指向用户提供语音和/或数据连通性的设备,具有无线连接功能的手持式设备、或连接到无线调制解调器的其他处理设备等。在不同的系统中,终端设备的名称可能也不相同,例如在5G系统中,终端设备可以称为用户设备(User Equipment,UE)。无线终端设备可以经无线接入网(Radio Access Network,RAN)与一个或多个核心网(Core Network,CN)进行通信,无线终端设备可以是移动终端设备,如移动电话(或称为“蜂窝”电话)和具有移动终端设备的计算机,例如,可以是便携式、袖珍式、手持式、计算机内置的或者车载的移动装置,它们与无线接入网交换语言和/或数据。例如,个人通信业务(Personal Communication Service,PCS)电话、无绳电话、会话发起协议(Session Initiated Protocol,SIP)话机、无线本地环路(Wireless Local Loop,WLL)站、个人数字助理(Personal Digital Assistant,PDA)等设备。无线终端设备也可以称为系

统、订户单元(subscriber unit)、订户站(subscriber station),移动站(mobile station)、移动台(mobile)、远程站(remote station)、接入点(access point)、远程终端设备(remote terminal)、接入终端设备(access terminal)、用户终端设备(user terminal)、用户代理(user agent)、用户装置(user device),本申请实施例中并不限定。

[0206] 如图14所示,本申请实施例的接入点认证装置,应用于CCU,包括:处理器1400,用于读取存储器1420中的程序,执行下列过程:

[0207] 获取第一AP的第二认证信息;

[0208] 从认证信息存储设备获取所述第一AP的第一认证信息;

[0209] 根据所述第二认证信息和所述第一认证信息对所述第一AP进行认证,得到认证结果;

[0210] 向终端发送所述认证结果。

[0211] 收发机1410,用于在处理器1400的控制下接收和发送数据。

[0212] 其中,在图14中,总线架构可以包括任意数量的互联的总线和桥,具体由处理器1400代表的一个或多个处理器和存储器1420代表的存储器的各种电路链接在一起。总线架构还可以将诸如外围设备、稳压器和功率管理电路等之类的各种其他电路链接在一起,这些都是本领域所公知的,因此,本文不再对其进行进一步描述。总线接口提供接口。收发机1410可以是多个元件,即包括发送机和接收机,提供用于在传输介质上与各种其他装置通信的单元。处理器1400负责管理总线架构和通常的处理,存储器1420可以存储处理器1400在执行操作时所使用的数据。

[0213] 处理器1400可以是中央处理器(CPU)、专用集成电路(Application Specific Integrated Circuit,ASIC)、现场可编程门阵列(Field—Programmable Gate Array,FPGA)或复杂可编程逻辑器件(Complex Programmable Logic Device,CPLD),处理器也可以采用多核架构。

[0214] 处理器1400负责管理总线架构和通常的处理,存储器1420可以存储处理器1400在执行操作时所使用的数据。

[0215] 可选的,所述第二认证信息包括第二数字证书或第二数字证书哈希值;处理器1400还用于读取所述程序,执行如下步骤:

[0216] 接收所述终端通过第二AP发送的第一请求,所述第一请求携带所述第二认证信息,所述第二认证信息包括所述第一AP的第二数字证书;或者

[0217] 接收所述终端通过第二AP发送的测量上报消息;根据所述测量上报消息从

[0218] 所述第一AP获取所述第一AP的第二数字证书;或者

[0219] 接收所述终端通过第二AP发送的所述第一请求,所述第一请求携带所述第二认证信息,所述第二认证信息包括所述第一AP的第二数字证书;确定所述第二数字证书的第二数字证书哈希值;

[0220] 其中,所述第二AP为已认证的AP。

[0221] 可选的,所述第一认证信息包括第一数字证书或第一数字证书哈希值;处理器1400还用于读取所述程序,执行如下步骤:

[0222] 从所述认证信息存储设备获取所述第一AP的第一数字证书;或者

[0223] 从所述认证信息存储设备获取所述第一AP的第一数字证书哈希值。

[0224] 可选的,所述第二认证信息包括所述第一AP的第二数字证书,所述第一认证信息包括所述第一AP的第一数字证书;处理器1400还用于读取所述程序,执行如下步骤:

[0225] 将所述第一数字证书和所述第二数字证书进行比较,得到所述认证结果。

[0226] 可选的,所述第二认证信息包括所述第一AP的第二数字证书哈希值,所述第一认证信息包括所述第一AP的第一数字证书哈希值;处理器1400还用于读取所述程序,执行如下步骤:

[0227] 将所述第一数字证书哈希值和所述第二数字证书哈希值进行比较,得到所述认证结果。

[0228] 处理器1400还用于读取所述程序,执行如下步骤:

[0229] 向所述认证信息存储设备存储所述CCU对应的域内的AP的数字证书和/或数字证书哈希值。

[0230] 在此需要说明的是,本申请实施例提供的上述装置,能够实现上述方法实施例所实现的所有方法步骤,且能够达到相同的技术效果,在此不再对本实施例中与方法实施例相同的部分及有益效果进行具体赘述。

[0231] 如图15所示,本申请实施例的接入点认证装置,应用于核心网设备,包括:处理器1500,用于读取存储器1520中的程序,执行下列过程:

[0232] 获取第一AP的第二认证信息;

[0233] 从认证信息存储设备获取所述第一AP的第一认证信息;

[0234] 根据所述第二认证信息和所述第一认证信息对所述第一AP进行认证,得到认证结果;

[0235] 向终端发送所述认证结果。

[0236] 收发机1510,用于在处理器1500的控制下接收和发送数据。

[0237] 其中,在图15中,总线架构可以包括任意数量的互联的总线和桥,具体由处理器1500代表的一个或多个处理器和存储器1520代表的存储器的各种电路链接在一起。总线架构还可以将诸如外围设备、稳压器和功率管理电路等之类的各种其他电路链接在一起,这些都是本领域所公知的,因此,本文不再对其进行进一步描述。总线接口提供接口。收发机1510可以是多个元件,即包括发送机和接收机,提供用于在传输介质上与各种其他装置通信的单元。处理器1500负责管理总线架构和通常的处理,存储器1520可以存储处理器1500在执行操作时所使用的数据。

[0238] 处理器1500可以是中央处理器(CPU)、专用集成电路(Application Specific Integrated Circuit,ASIC)、现场可编程门阵列(Field—Programmable Gate Array,FPGA)或复杂可编程逻辑器件(Complex Programmable Logic Device,CPLD),处理器也可以采用多核架构。

[0239] 处理器1500负责管理总线架构和通常的处理,存储器1520可以存储处理器1500在执行操作时所使用的数据。

[0240] 可选的,所述第二认证信息包括第二数字证书或第二数字证书哈希值;处理器1500还用于读取所述程序,执行如下步骤:

[0241] 接收所述终端通过第二AP发送的第一请求,所述第一请求携带所述第二认证信息,所述第二认证信息包括所述第一AP的第二数字证书;或者

[0242] 接收所述终端通过第二AP发送的所述第一请求,所述第一请求携带所述第二认证信息,所述第二认证信息包括所述第一AP的第二数字证书;确定所述第二数字证书的第二数字证书哈希值;

[0243] 其中,所述第二AP为已认证的AP。

[0244] 可选的,所述第一认证信息包括第一数字证书或第一数字证书哈希值;处理器1500还用于读取所述程序,执行如下步骤:

[0245] 从所述认证信息存储设备获取所述第一AP的第一数字证书;或者

[0246] 从所述认证信息存储设备获取所述第一AP的第一数字证书哈希值。

[0247] 可选的,所述第二认证信息包括所述第一AP的第二数字证书,所述第一认证信息包括所述第一AP的第一数字证书;处理器1500还用于读取所述程序,执行如下步骤:

[0248] 将所述第一数字证书和所述第二数字证书进行比较,得到所述认证结果。

[0249] 可选的,所述第二认证信息包括所述第一AP的第二数字证书哈希值,所述第一认证信息包括所述第一AP的第一数字证书哈希值;处理器1500还用于读取所述程序,执行如下步骤:

[0250] 将所述第一数字证书哈希值和所述第二数字证书哈希值进行比较,得到所述认证结果。

[0251] 可选的,处理器1500还用于读取所述程序,执行如下步骤:

[0252] 向所述认证信息存储设备存储所述核心网设备对应的域内的AP的数字证书和/或数字证书哈希值。

[0253] 在此需要说明的是,本申请实施例提供的上述装置,能够实现上述方法实施例所实现的所有方法步骤,且能够达到相同的技术效果,在此不再对本实施例中与方法实施例相同的部分及有益效果进行具体赘述。

[0254] 如图16所示,本申请实施例的接入点认证装置,应用于第一AP,包括:处理器1600,用于读取存储器1620中的程序,执行下列过程:

[0255] 向终端发送第二请求,所述第二请求用于表示所述第一AP为待认证的AP;

[0256] 向所述终端或CCU发送第二认证信息,所述第二认证信息用于通过所述终端发送给所述CCU或核心网设备,或者直接发送给所述CCU,并由所述CCU或所述核心网设备根据从认证信息存储设备获取的第一认证信息对所述第一AP进行认证。

[0257] 收发机1610,用于在处理器1600的控制下接收和发送数据。

[0258] 其中,在图16中,总线架构可以包括任意数量的互联的总线和桥,具体由处理器1600代表的一个或多个处理器和存储器1620代表的存储器的各种电路链接在一起。总线架构还可以将诸如外围设备、稳压器和功率管理电路等之类的各种其他电路链接在一起,这些都是本领域所公知的,因此,本文不再对其进行进一步描述。总线接口提供接口。收发机1610可以是多个元件,即包括发送机和接收机,提供用于在传输介质上与各种其他装置通信的单元。处理器1600负责管理总线架构和通常的处理,存储器1620可以存储处理器1600在执行操作时所使用的数据。

[0259] 处理器1600可以是中央处理器(CPU)、专用集成电路(Application Specific Integrated Circuit,ASIC)、现场可编程门阵列(Field—Programmable Gate Array,FPGA)或复杂可编程逻辑器件(Complex Programmable Logic Device,CPLD),处理器也可

以采用多核架构。

[0260] 处理器1600负责管理总线架构和通常的处理,存储器1620可以存储处理器1600在执行操作时所使用的数据。

[0261] 处理器1600还用于读取所述程序,执行如下步骤:

[0262] 接收所述CCU的第三请求;

[0263] 响应于所述第三请求,向所述CCU发送所述第二认证信息;所述第二认证信息包括所述第一AP的第二数字证书。

[0264] 在此需要说明的是,本申请实施例提供的上述装置,能够实现上述方法实施例所实现的所有方法步骤,且能够达到相同的技术效果,在此不再对本实施例中与方法实施例相同的部分及有益效果进行具体赘述。

[0265] 如图17所示,本申请实施例的接入点认证装置,应用于终端,包括:处理器1700,用于读取存储器1720中的程序,执行下列过程:

[0266] 向CCU或核心网设备发送第一请求,所述第一请求用于请求所述CCU或者所述核心网设备对第一接入点AP进行认证;

[0267] 接收所述CCU或所述核心网设备发送的所述第一AP的认证结果;

[0268] 其中,所述认证结果是由所述CCU或所述核心网设备根据从认证信息存储设备获取的第一认证信息对所述第一AP进行认证得到的。

[0269] 收发机1710,用于在处理器1700的控制下接收和发送数据。

[0270] 其中,在图17中,总线架构可以包括任意数量的互联的总线和桥,具体由处理器1700代表的一个或多个处理器和存储器1720代表的存储器的各种电路链接在一起。总线架构还可以将诸如外围设备、稳压器和功率管理电路等之类的各种其他电路链接在一起,这些都是本领域所公知的,因此,本文不再对其进行进一步描述。总线接口提供接口。收发机1710可以是多个元件,即包括发送机和接收机,提供用于在传输介质上与各种其他装置通信的单元。针对不同的用户设备,用户接口1730还可以是能够外接内接需要设备的接口,连接的设备包括但不限于小键盘、显示器、扬声器、麦克风、操纵杆等。

[0271] 处理器1700负责管理总线架构和通常的处理,存储器1720可以存储处理器1700在执行操作时所使用的数据。

[0272] 处理器1700可以是中央处理器(CPU)、专用集成电路(Application Specific Integrated Circuit,ASIC)、现场可编程门阵列(Field—Programmable Gate Array,FPGA)或复杂可编程逻辑器件(Complex Programmable Logic Device,CPLD),处理器也可以采用多核架构。

[0273] 处理器通过调用存储器存储的计算机程序,用于按照获得的可执行指令执行本申请实施例提供的任一所述方法。处理器与存储器也可以物理上分开布置。

[0274] 处理器1700还用于读取所述程序,执行如下步骤:

[0275] 通过第二AP向所述CCU或所述核心网设备发送所述第一请求,所述第一请求携带第二认证信息,所述第二认证信息包括所述第一AP的第二数字证书;或者

[0276] 通过第二AP向所述CCU发送测量上报消息,所述第一请求包括所述测量上报消息;

[0277] 其中,所述第二AP为已认证的AP。

[0278] 处理器1700还用于读取所述程序,执行如下步骤:

[0279] 从所述第一AP获取所述第二数字证书。

[0280] 在此需要说明的是,本申请实施例提供的上述装置,能够实现上述方法实施例所实现的所有方法步骤,且能够达到相同的技术效果,在此不再对本实施例中与方法实施例相同的部分及有益效果进行具体赘述。

[0281] 如图18所示,本申请实施例的接入点认证装置,应用于终端,包括:

[0282] 第一发送单元1801,用于向CCU或核心网设备发送第一请求,所述第一请求用于请求所述CCU或者所述核心网设备对第一接入点AP进行认证;第一接收单元1802,用于接收所述CCU或所述核心网设备发送的所述第一AP的认证结果;

[0283] 其中,所述认证结果是由所述CCU或所述核心网设备根据从认证信息存储设备获取的第一认证信息对所述第一AP进行认证得到的。

[0284] 可选的,所述第一发送单元用于:

[0285] 通过第二AP向所述CCU或所述核心网设备发送所述第一请求,所述第一请求携带第二认证信息,所述第二认证信息包括所述第一AP的第二数字证书;或者

[0286] 通过第二AP向所述CCU发送测量上报消息,所述第一请求包括所述测量上报消息;

[0287] 其中,所述第二AP为已认证的AP。

[0288] 可选的,所述装置还可包括:

[0289] 第一获取单元,用于从所述第一AP获取所述第二数字证书。

[0290] 在此需要说明的是,本申请实施例提供的上述装置,能够实现上述方法实施例所实现的所有方法步骤,且能够达到相同的技术效果,在此不再对本实施例中与方法实施例相同的部分及有益效果进行具体赘述。

[0291] 如图19所示,本申请实施例的接入点认证装置,应用于CCU,包括:

[0292] 第一获取单元1901,用于获取第一AP的第二认证信息;第二获取单元1902,用于从认证信息存储设备获取所述第一AP的第一认证信息;第一认证单元1903,用于根据所述第二认证信息和所述第一认证信息对所述第一AP进行认证,得到认证结果;第一发送单元1904,用于向终端发送所述认证结果。

[0293] 可选的,所述第二认证信息包括第二数字证书或第二数字证书哈希值;所述第一获取单元用于:

[0294] 接收所述终端通过第二AP发送的第一请求,所述第一请求携带所述第二认证信息,所述第二认证信息包括所述第一AP的第二数字证书;或者

[0295] 接收所述终端通过第二AP发送的测量上报消息;根据所述测量上报消息从所述第一AP获取所述第一AP的第二数字证书;或者

[0296] 接收所述终端通过第二AP发送的所述第一请求,所述第一请求携带所述第二认证信息,所述第二认证信息包括所述第一AP的第二数字证书;确定所述第二数字证书的第二数字证书哈希值;

[0297] 其中,所述第二AP为已认证的AP。

[0298] 可选的,所述第一认证信息包括第一数字证书或第一数字证书哈希值;所述第二获取单元用于:

[0299] 从所述认证信息存储设备获取所述第一AP的第一数字证书;或者

[0300] 从所述认证信息存储设备获取所述第一AP的第一数字证书哈希值。

[0301] 可选的,所述第二认证信息包括所述第一AP的第二数字证书,所述第一认证信息包括所述第一AP的第一数字证书;所述第一认证单元,用于:将所述第一数字证书和所述第二数字证书进行比较,得到所述认证结果。

[0302] 可选的,所述第二认证信息包括所述第一AP的第二数字证书哈希值,所述第一认证信息包括所述第一AP的第一数字证书哈希值;所述第一认证单元,用于:将所述第一数字证书哈希值和所述第二数字证书哈希值进行比较,得到所述认证结果。

[0303] 可选的,所述装置还可包括:

[0304] 存储单元,用于向所述认证信息存储设备存储所述CCU对应的域内的AP的数字证书和/或数字证书哈希值。

[0305] 在此需要说明的是,本申请实施例提供的上述装置,能够实现上述方法实施例所实现的所有方法步骤,且能够达到相同的技术效果,在此不再对本实施例中与方法实施例相同的部分及有益效果进行具体赘述。

[0306] 如图20所示,本申请实施例的接入点认证装置,应用于核心网设备,包括:

[0307] 第一获取单元2001,用于获取第一AP的第二认证信息;第二获取单元2002,用于从认证信息存储设备获取所述第一AP的第一认证信息;第一认证单元2003,用于根据所述第二认证信息和所述第一认证信息对所述第一AP进行认证,得到认证结果;第一发送单元2004,用于向终端发送所述认证结果。

[0308] 可选的,所述第二认证信息包括第二数字证书或第二数字证书哈希值;所述第一获取单元用于:

[0309] 接收所述终端通过第二AP发送的第一请求,所述第一请求携带所述第二认证信息,所述第二认证信息包括所述第一AP的第二数字证书;或者

[0310] 接收所述终端通过第二AP发送的所述第一请求,所述第一请求携带所述第二认证信息,所述第二认证信息包括所述第一AP的第二数字证书;确定所述第二数字证书的第二数字证书哈希值;

[0311] 其中,所述第二AP为已认证的AP。

[0312] 可选的,所述第一认证信息包括第一数字证书或第一数字证书哈希值;所述第二获取单元用于:

[0313] 从所述认证信息存储设备获取所述第一AP的第一数字证书;或者

[0314] 从所述认证信息存储设备获取所述第一AP的第一数字证书哈希值。

[0315] 可选的,所述第二认证信息包括所述第一AP的第二数字证书,所述第一认证信息包括所述第一AP的第一数字证书;所述第一认证单元,用于:将所述第一数字证书和所述第二数字证书进行比较,得到所述认证结果。

[0316] 可选的,所述第二认证信息包括所述第一AP的第二数字证书哈希值,所述第一认证信息包括所述第一AP的第一数字证书哈希值;所述第一认证单元,用于:将所述第一数字证书哈希值和所述第二数字证书哈希值进行比较,得到所述认证结果。

[0317] 可选的,所述装置还可包括:

[0318] 存储单元,用于向所述认证信息存储设备存储所述核心网设备对应的域内的AP的数字证书和/或数字证书哈希值。

[0319] 在此需要说明的是,本申请实施例提供的上述装置,能够实现上述方法实施例所

实现的所有方法步骤,且能够达到相同的技术效果,在此不再对本实施例中与方法实施例相同的部分及有益效果进行具体赘述。

[0320] 如图21所示,本申请实施例的接入点认证装置,应用于第一AP,包括:

[0321] 第一发送单元2101,用于向终端发送第二请求,所述第二请求用于表示所述第一AP为待认证的AP;第二发送单元2102,用于向所述终端或CCU发送第二认证信息,所述第二认证信息用于通过所述终端发送给所述CCU或核心网设备,或者直接发送给所述CCU,并由所述CCU或所述核心网设备根据从认证信息存储设备获取的第一认证信息对所述第一AP进行认证。

[0322] 可选的,所述第二发送单元,用于:接收所述CCU的第三请求;响应于所述第三请求,向所述CCU发送所述第二认证信息;所述第二认证信息包括所述第一AP的第二数字证书。

[0323] 在此需要说明的是,本申请实施例提供的上述装置,能够实现上述方法实施例所实现的所有方法步骤,且能够达到相同的技术效果,在此不再对本实施例中与方法实施例相同的部分及有益效果进行具体赘述。

[0324] 需要说明的是,本申请实施例中对单元的划分是示意性的,仅仅为一种逻辑功能划分,实际实现时可以有另外的划分方式。另外,在本申请各个实施例中的各功能单元可以集成在一个处理单元中,也可以是各个单元单独物理存在,也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现,也可以采用软件功能单元的形式实现。

[0325] 所述集成的单元如果以软件功能单元的形式实现并作为独立的产品销售或使用时,可以存储在一个处理器可读取存储介质中。基于这样的理解,本申请的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的全部或部分可以以软件产品的形式体现出来,该计算机软件产品存储在一个存储介质中,包括若干指令用以使得一台计算机设备(可以是个人计算机,服务器,或者网络设备等)或处理器(processor)执行本申请各个实施例所述方法的全部或部分步骤。而前述的存储介质包括:U盘、移动硬盘、只读存储器(Read-Only Memory,ROM)、随机存取存储器(Random Access Memory,RAM)、磁碟或者光盘等各种可以存储程序代码的介质。

[0326] 本申请实施例还提供一种处理器可读存储介质,可读存储介质上存储有程序,该程序被处理器执行时实现上述接入点认证方法实施例的各个过程,且能达到相同的技术效果,为避免重复,这里不再赘述。其中,所述的可读存储介质,可以是处理器能够存取的任何可用介质或数据存储设备,包括但不限于磁性存储器(例如软盘、硬盘、磁带、磁光盘(MO)等)、光学存储器(例如CD、DVD、BD、HVD等)、以及半导体存储器(例如ROM、EPROM、EEPROM、非易失性存储器(NAND FLASH)、固态硬盘(SSD))等。

[0327] 需要说明的是,在本文中,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、物品或者装置不仅包括那些要素,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、物品或者装置所固有的要素。在没有更多限制的情况下,由语句“包括一个……”限定的要素,并不排除在包括该要素的过程、方法、物品或者装置中还存在另外的相同要素。

[0328] 通过以上的实施方式的描述,本领域的技术人员可以清楚地了解到上述实施例方

法可借助软件加必需的通用硬件平台的方式来实现,当然也可以通过硬件,但很多情况下前者是更佳的实施方式。根据这样的理解,本申请的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来,该计算机软件产品存储在一个存储介质(如ROM/RAM、磁盘、光盘)中,包括若干指令用以使得一台终端(可以是手机,计算机,服务器,空调器,或者网络设备等)执行本申请各个实施例所述的方法。

[0329] 上面结合附图对本申请的实施例进行了描述,但是本申请并不局限于上述的具体实施方式,上述的具体实施方式仅仅是示意性的,而不是限制性的,本领域的普通技术人员在本申请的启示下,在不脱离本申请宗旨和权利要求所保护的范围情况下,还可做出很多形式,均属于本申请的保护之内。

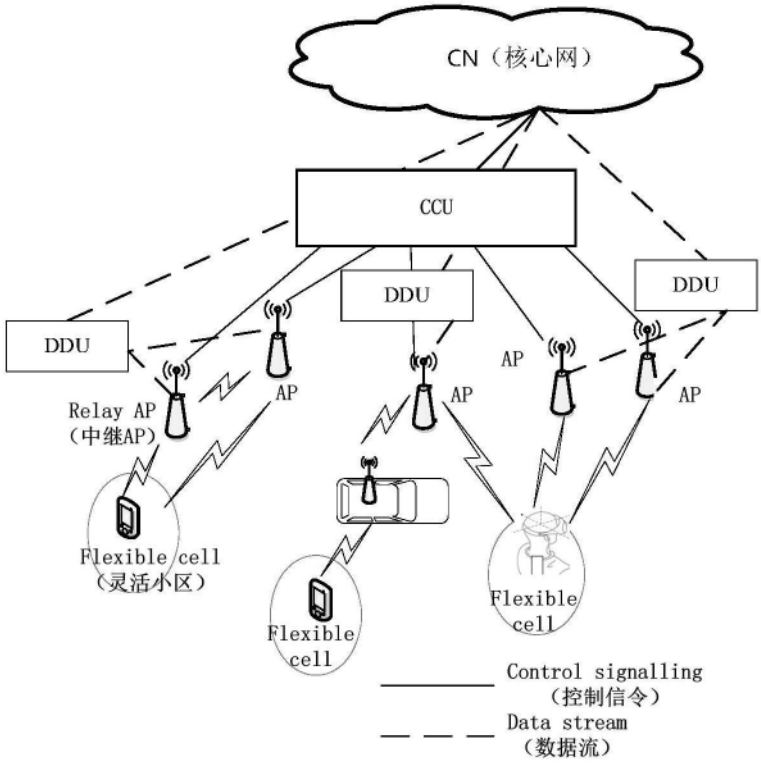

CN（核心网）
CCU
DDU
DDU
DDU
AP
AP
AP
AP
Relay AP
（中继AP）
Flexible cell
（灵活小区）
Flexible
cell
Flexible
cell
Control signalling
（控制信令）
Data stream
（数据流）

图1

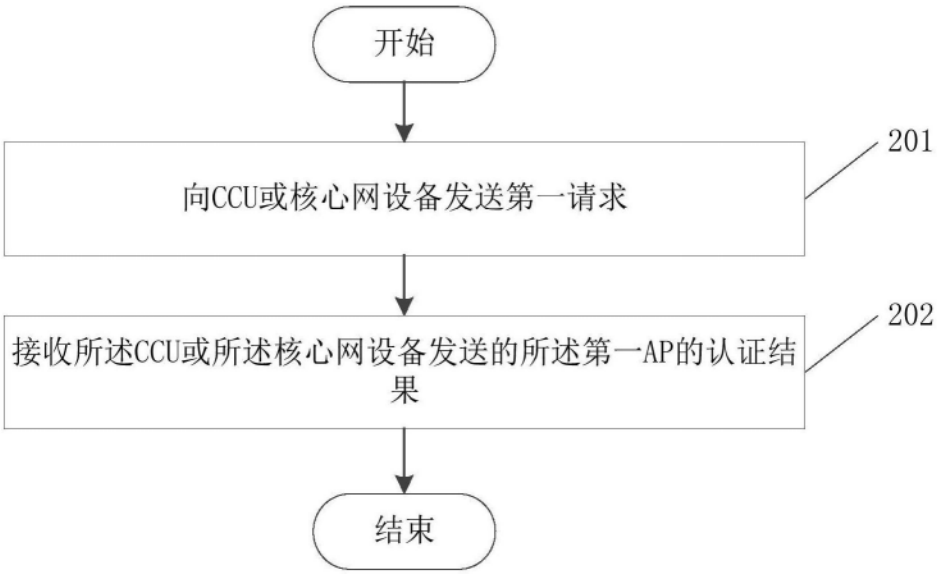

开始
向CCU或核心网设备发送第一请求
201
接收所述CCU或所述核心网设备发送的所述第一AP的认证结果
202
结束

图2

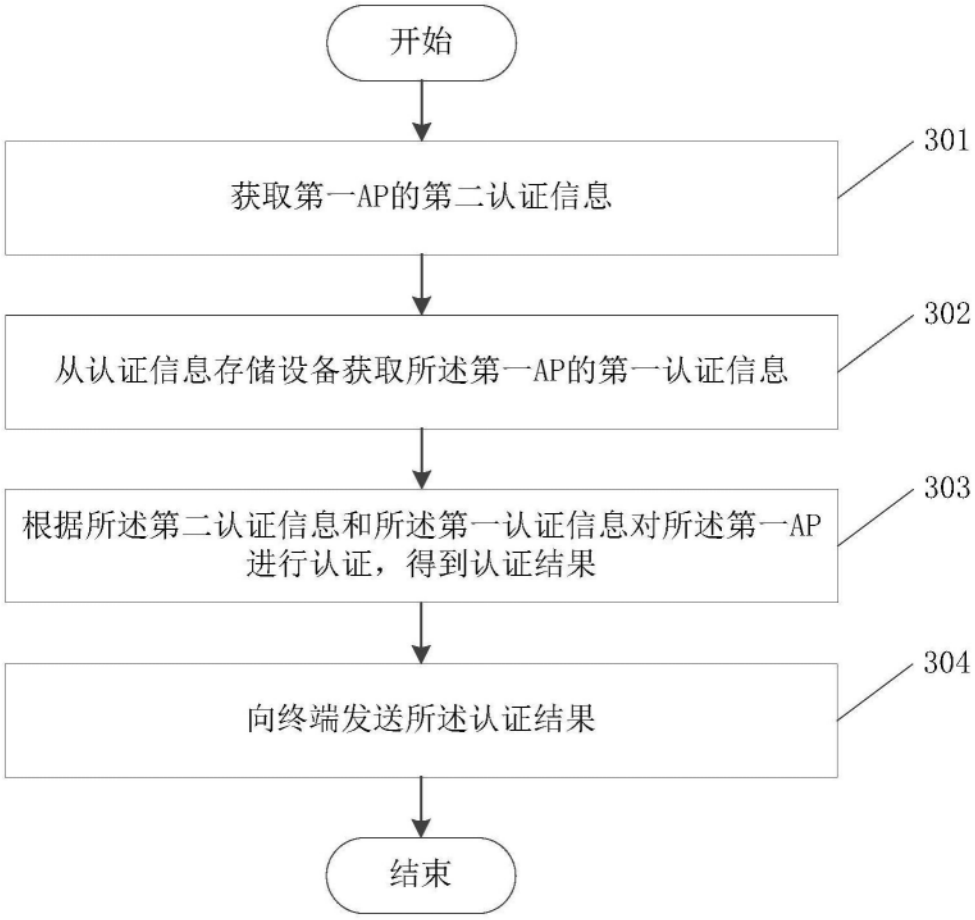

开始
301
获取第一AP的第二认证信息
302
从认证信息存储设备获取所述第一AP的第一认证信息
303
根据所述第二认证信息和所述第一认证信息对所述第一AP进行认证，得到认证结果
304
向终端发送所述认证结果
结束

图3

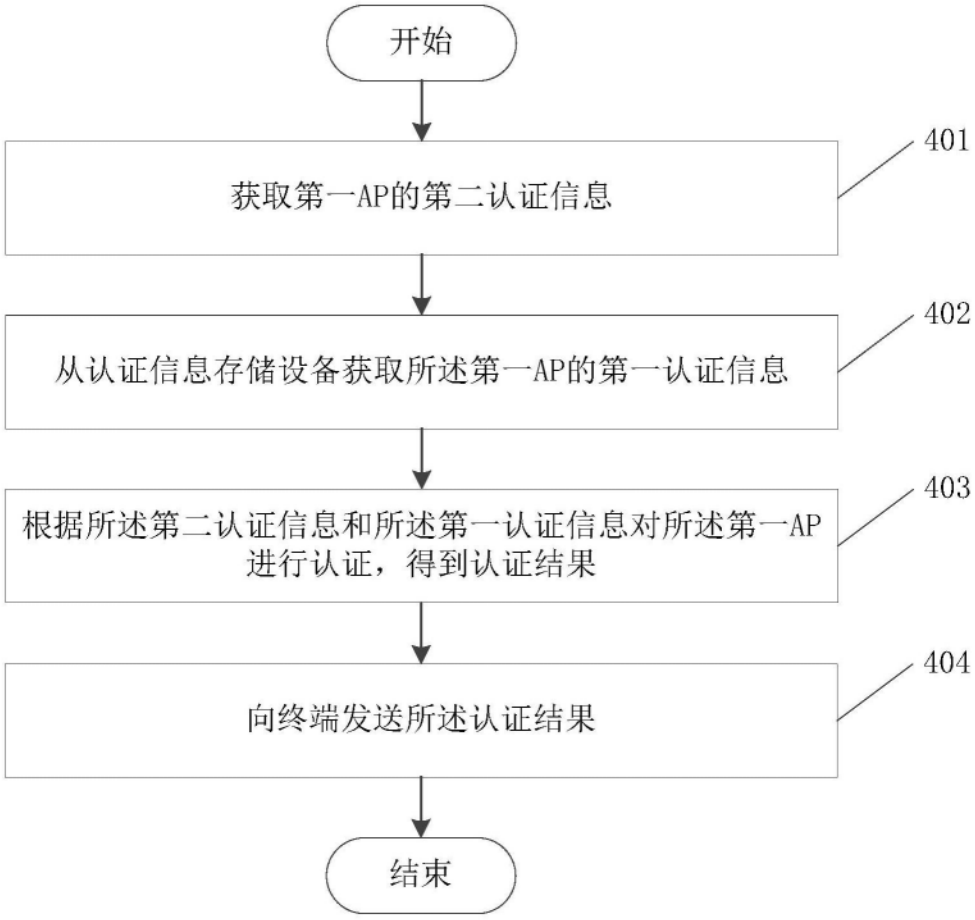

开始
401
获取第一AP的第二认证信息
402
从认证信息存储设备获取所述第一AP的第一认证信息
403
根据所述第二认证信息和所述第一认证信息对所述第一AP进行认证，得到认证结果
404
向终端发送所述认证结果
结束

图4

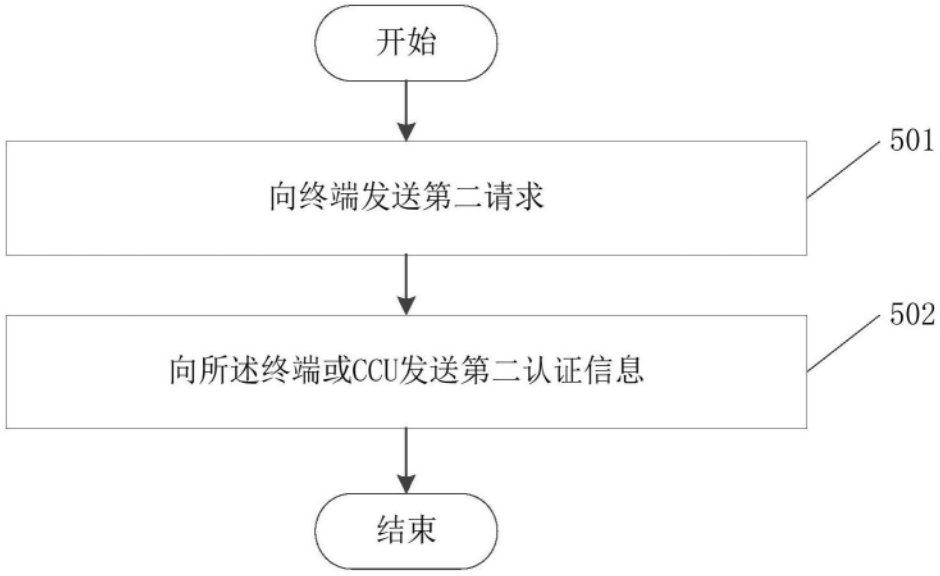

开始
501
向终端发送第二请求
502
向所述终端或CCU发送第二认证信息
结束

图5

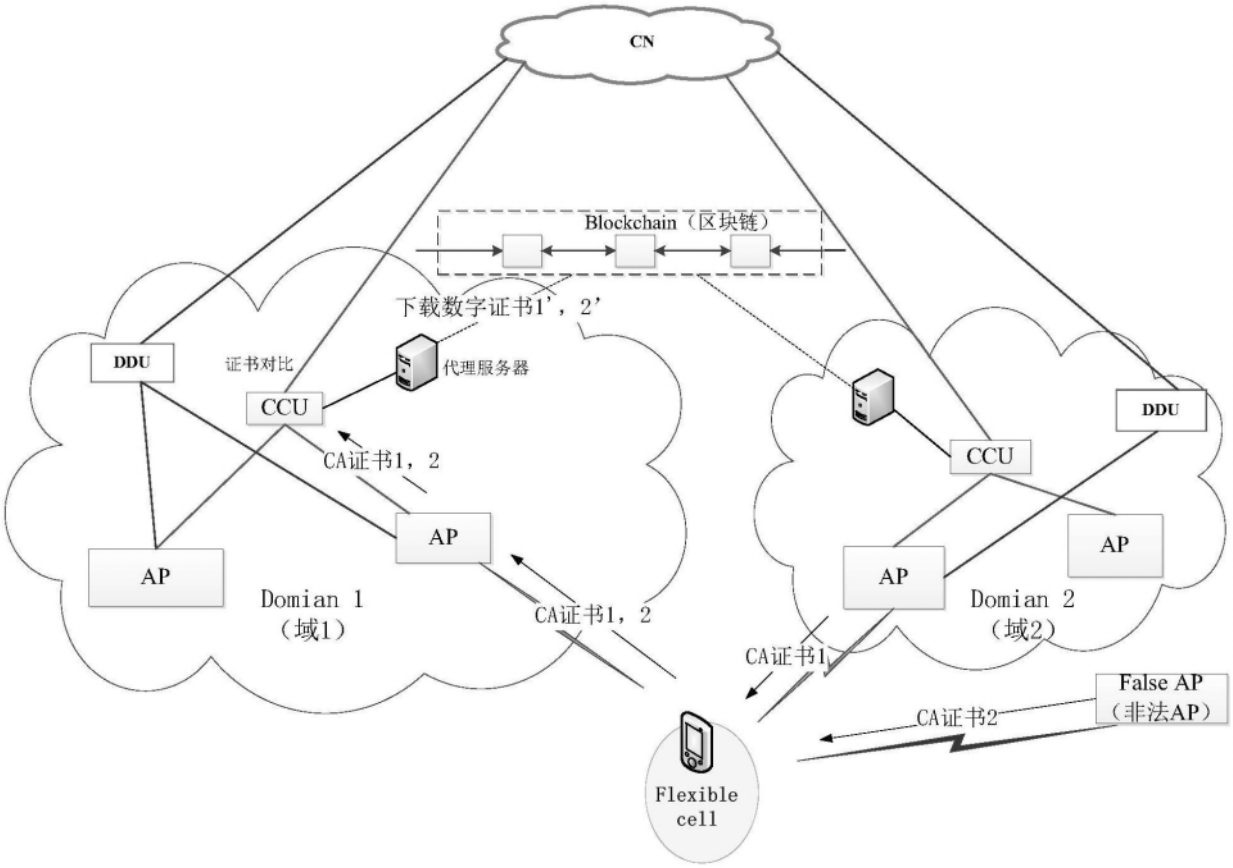

CN
Blockchain（区块链）
下载数字证书1'，2'
DDU
证书对比
代理服务器
CCU
CA证书1，2
AP
AP
Domian 1
（域1）
CA证书1，2
CCU
DDU
AP
AP
Domian 2
（域2）
CA证书1
False AP
（非法AP）
CA证书2
Flexible
cell

图6

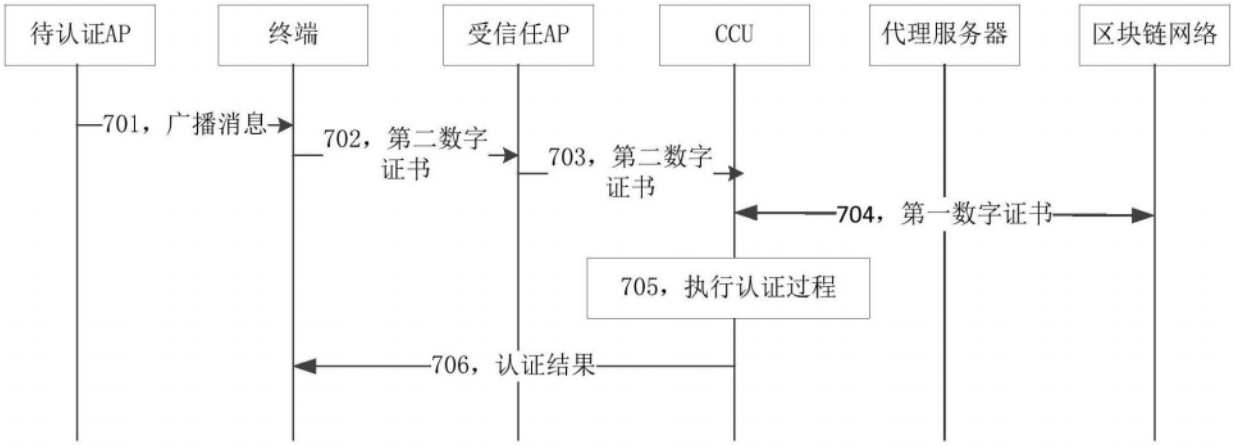

待认证AP
终端
受信任AP
CCU
代理服务器
区块链网络
701，广播消息
702，第二数字证书
703，第二数字证书
704，第一数字证书
705，执行认证过程
706，认证结果

图7

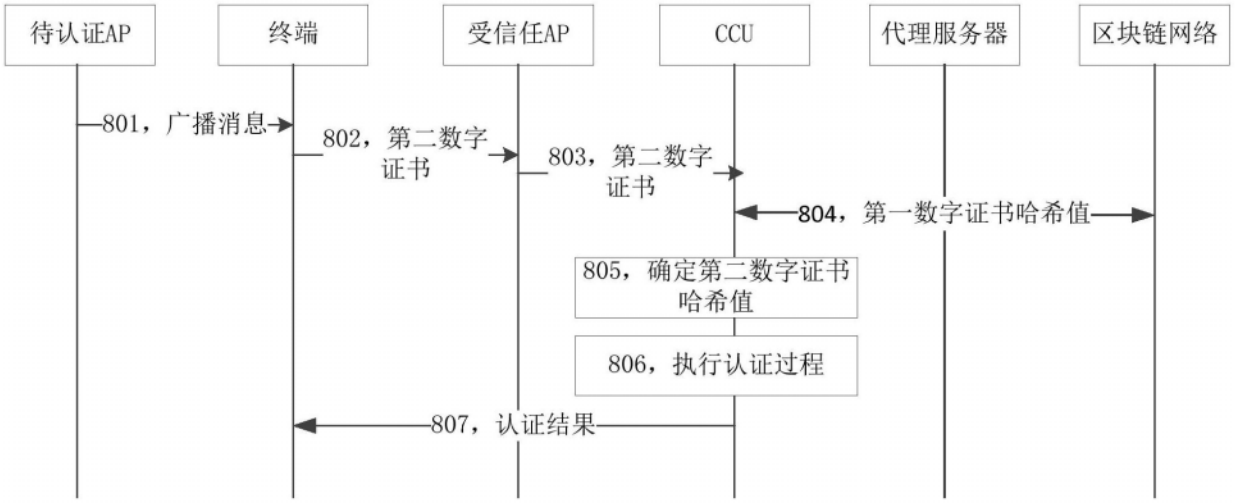

待认证AP
终端
受信任AP
CCU
代理服务器
区块链网络
801，广播消息
802，第二数字证书
803，第二数字证书
804，第一数字证书哈希值
805，确定第二数字证书哈希值
806，执行认证过程
807，认证结果

图8

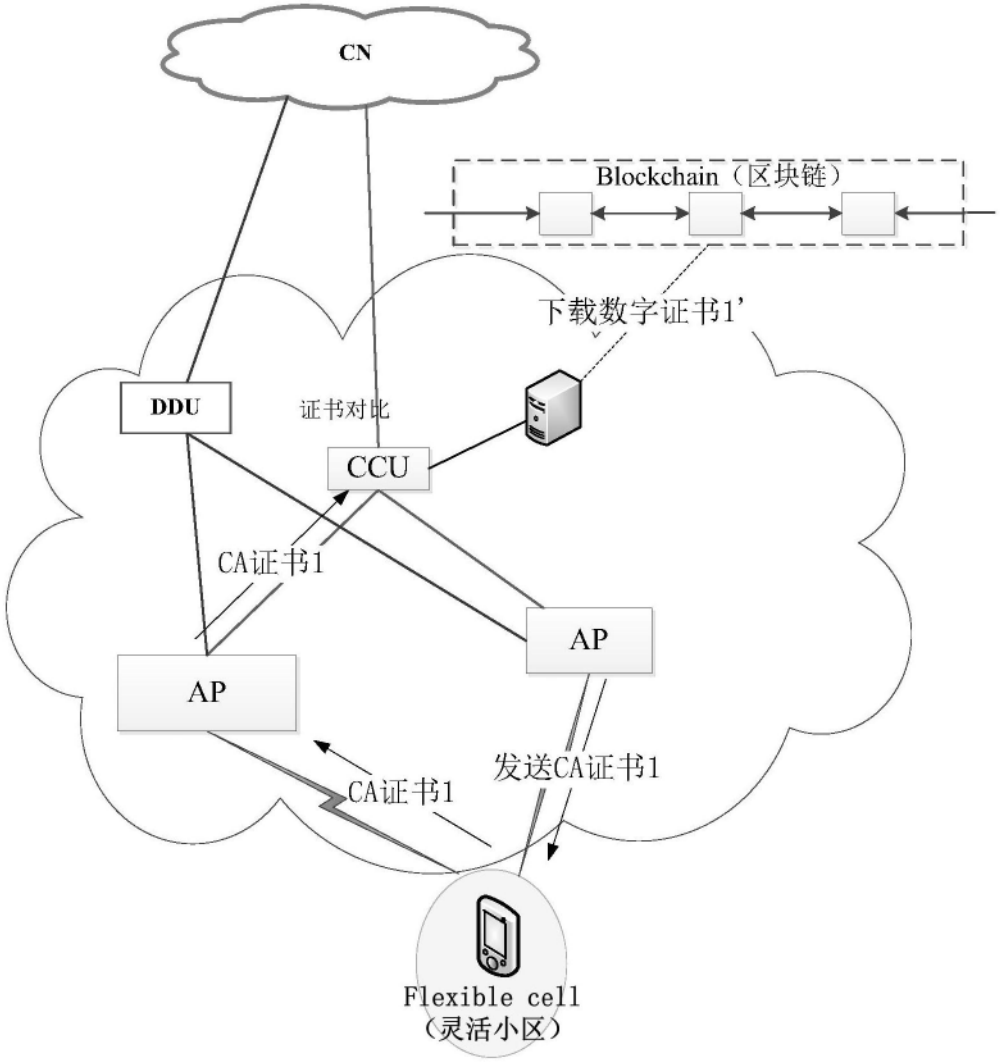

CN
Blockchain（区块链）
下载数字证书1'
DDU
证书对比
CCU
CA证书1
AP
AP
发送CA证书1
CA证书1
Flexible cell
（灵活小区）

图9

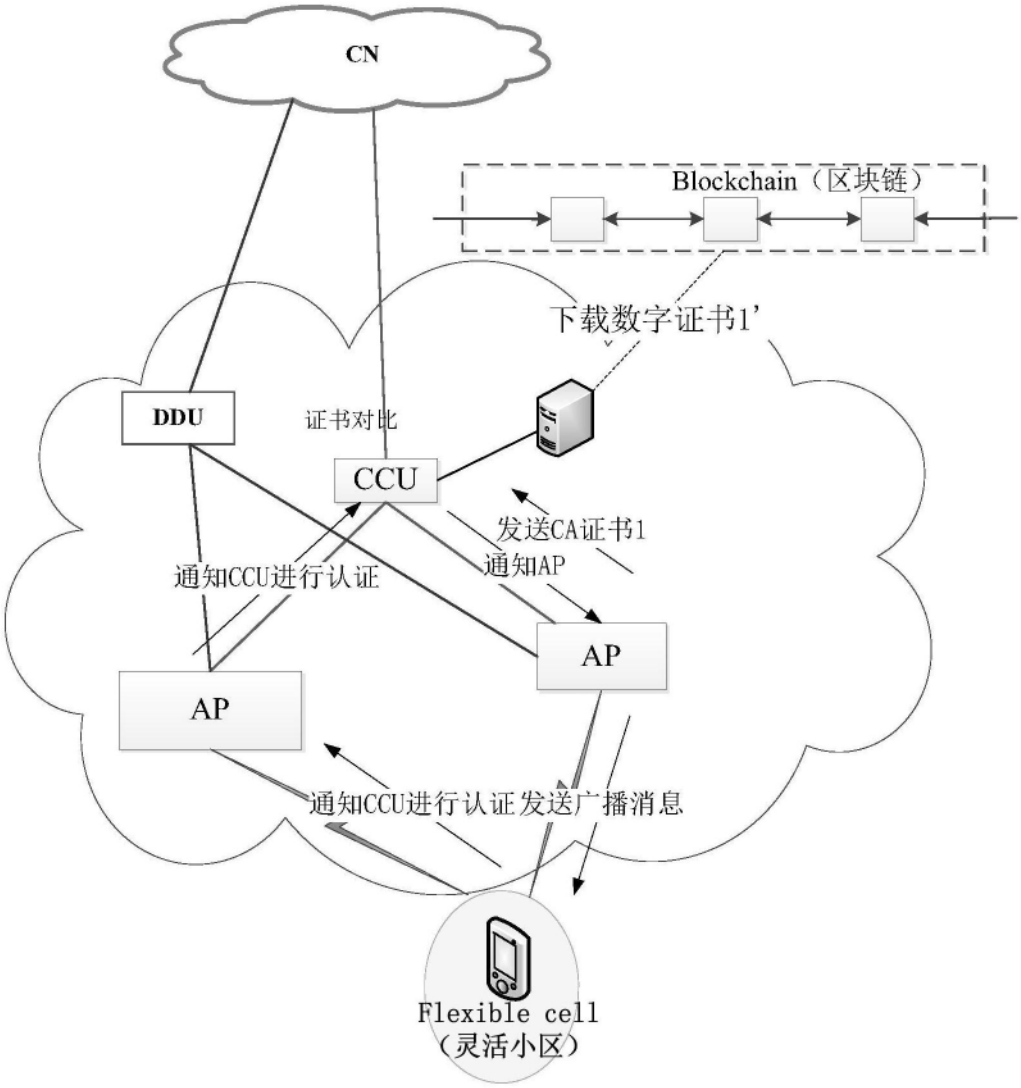

CN
Blockchain（区块链）
下载数字证书1'
DDU
证书对比
CCU
发送CA证书1
通知AP
通知CCU进行认证
AP
AP
通知CCU进行认证发送广播消息
Flexible cell
（灵活小区）

图10

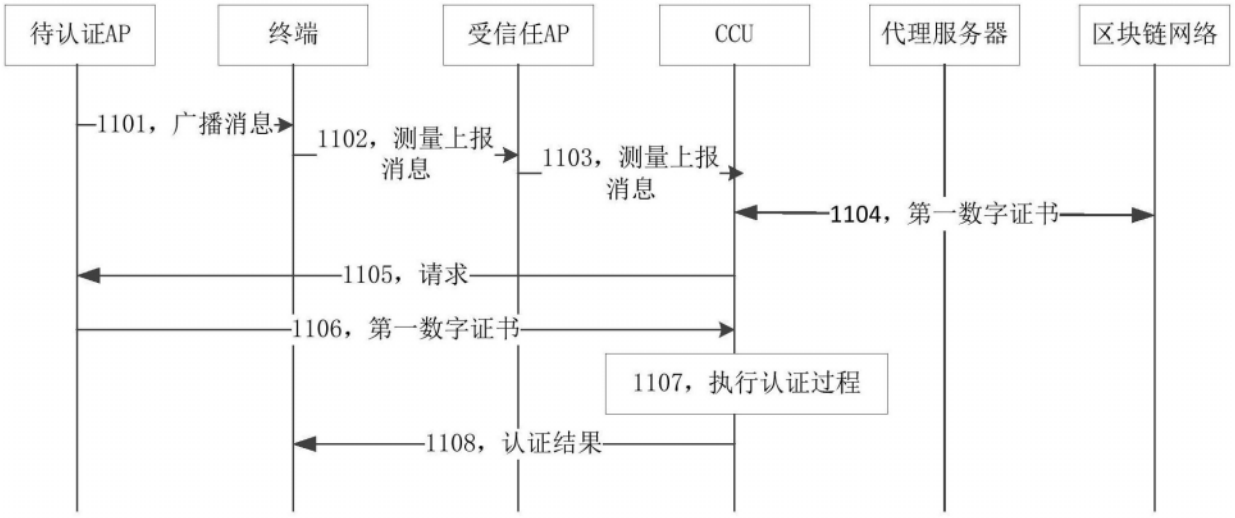

待认证AP
终端
受信任AP
CCU
代理服务器
区块链网络
1101，广播消息
1102，测量上报消息
1103，测量上报消息
1104，第一数字证书
1105，请求
1106，第一数字证书
1107，执行认证过程
1108，认证结果

图11

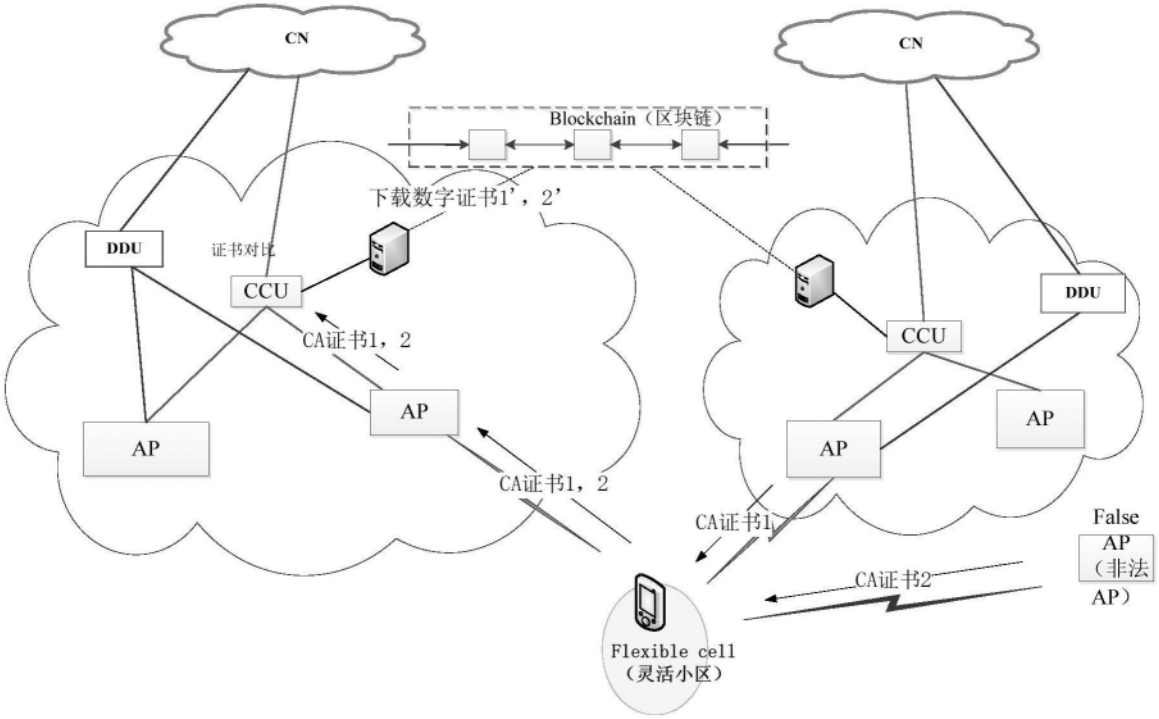

CN
CN
Blockchain（区块链）
下载数字证书1'，2'
DDU
证书对比
CCU
CA证书1，2
AP
AP
CA证书1，2
CA证书1
CCU
DDU
AP
AP
False
AP
（非法
AP）
CA证书2
Flexible cell
（灵活小区）

图12

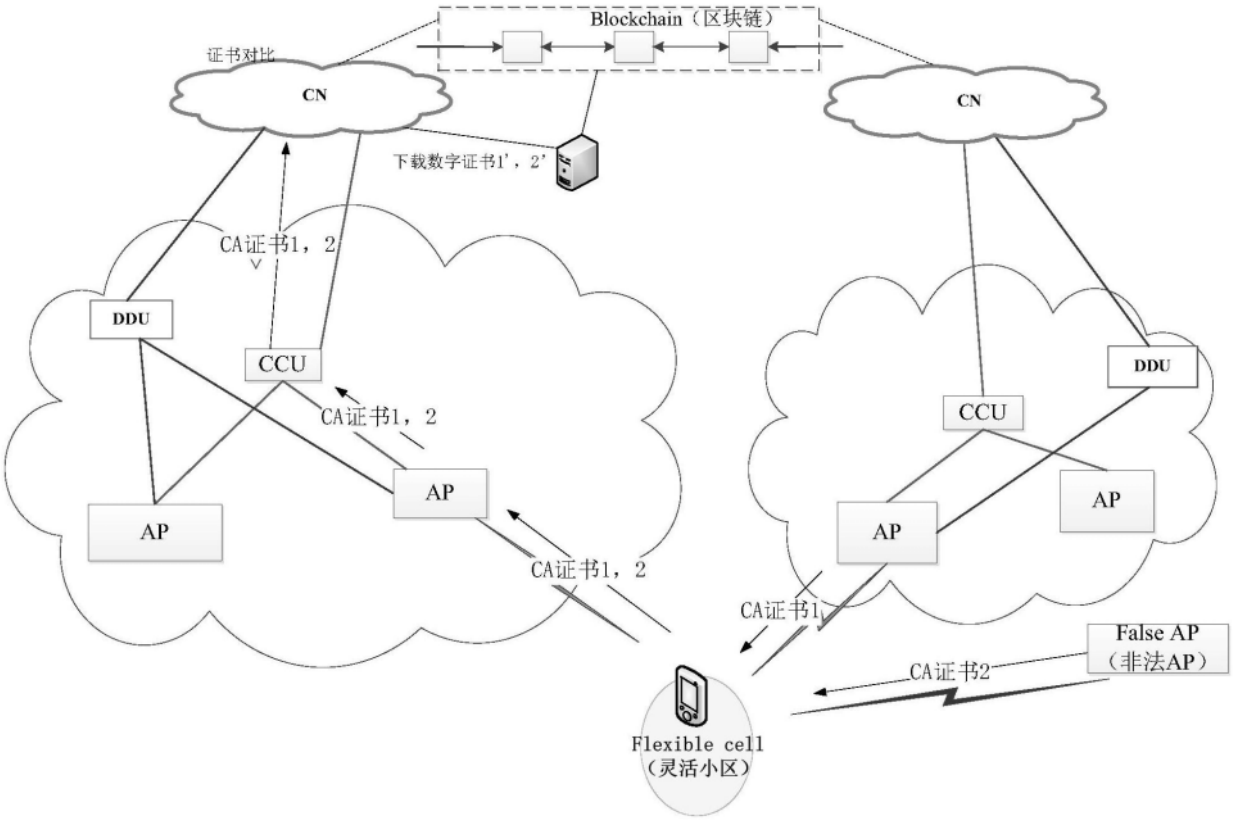

Blockchain（区块链）
证书对比
CN
CN
下载数字证书1'，2'
CA证书1，2
DDU
CCU
CA证书1，2
AP
AP
CA证书1，2
DDU
CCU
AP
AP
CA证书1
False AP
（非法AP）
CA证书2
Flexible cell
（灵活小区）

图13(a)

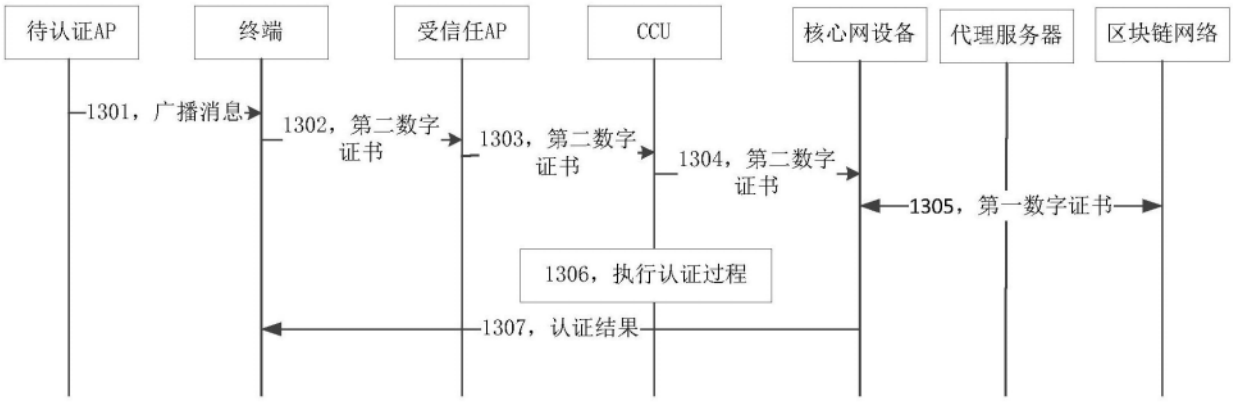

待认证AP
终端
受信任AP
CCU
核心网设备
代理服务器
区块链网络
1301，广播消息
1302，第二数字证书
1303，第二数字证书
1304，第二数字证书
1305，第一数字证书
1306，执行认证过程
1307，认证结果

图13(b)

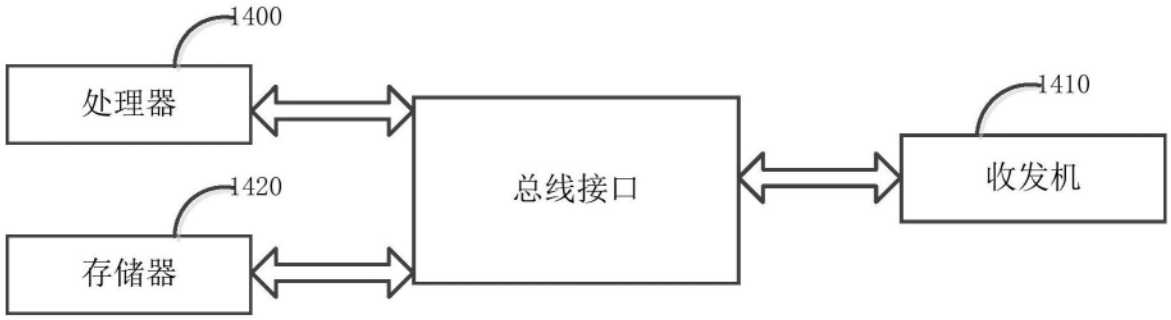

1400
处理器
1420
存储器
总线接口
1410
收发机

图14

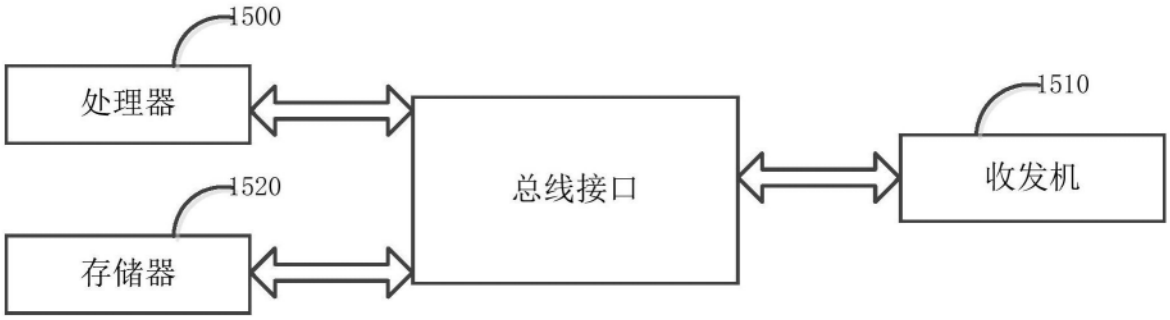

1500
处理器
1520
存储器
总线接口
1510
收发机

图15

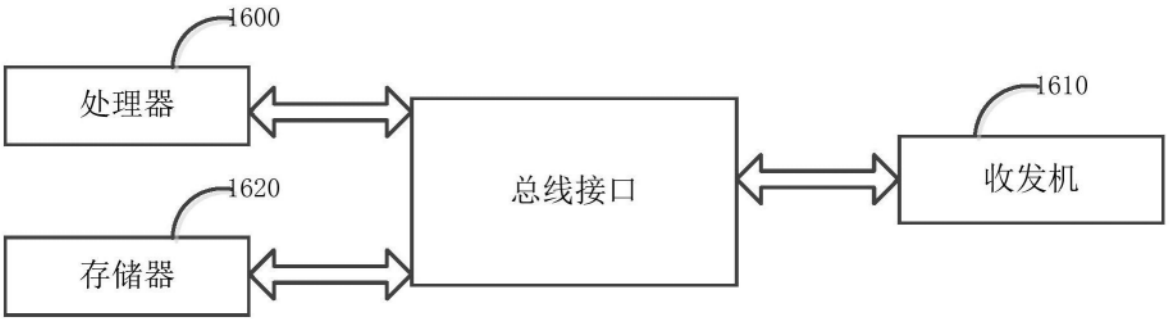

1600
处理器
1620
存储器
总线接口
1610
收发机

图16

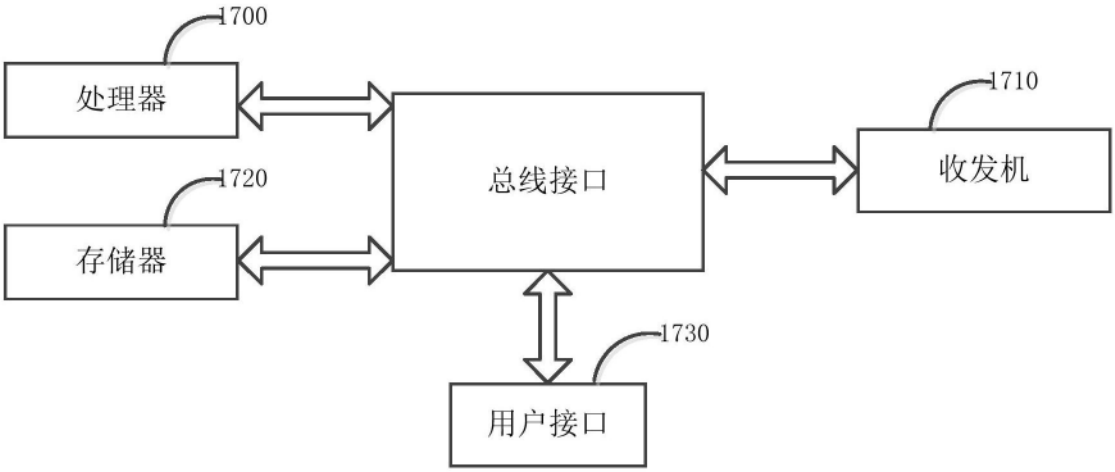

1700
处理器
1720
存储器
总线接口
1710
收发机
1730
用户接口

图17

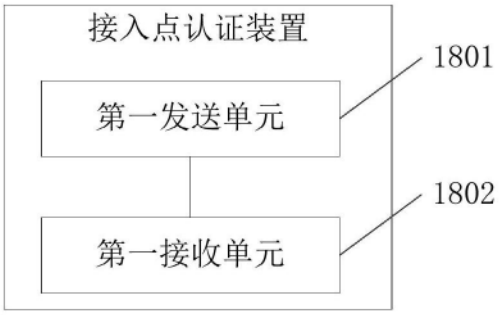

接入点认证装置
1801
第一发送单元
1802
第一接收单元

图18

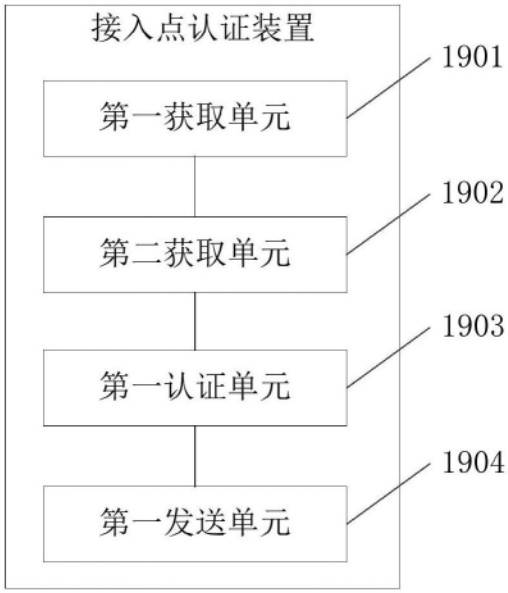

接入点认证装置
1901
第一获取单元
1902
第二获取单元
1903
第一认证单元
1904
第一发送单元

图19

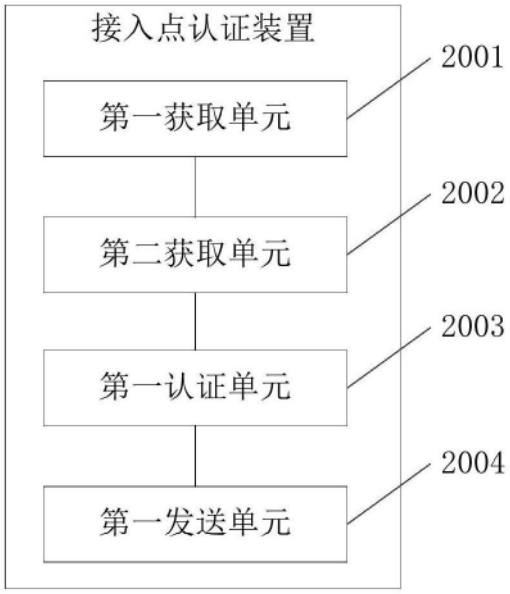

接入点认证装置
2001
第一获取单元
2002
第二获取单元
2003
第一认证单元
2004
第一发送单元

图20

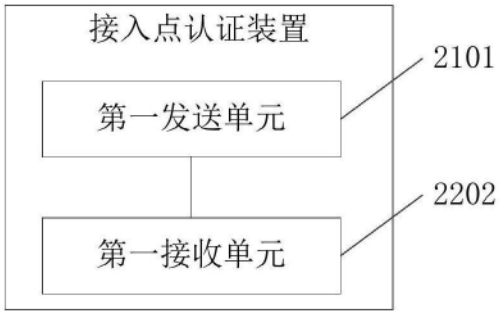

接入点认证装置
2101
第一发送单元
2202
第一接收单元

图21