(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 2 月 21 日 (21.02.2019)

WIPO | PCT

(10) 国际公布号
WO 2019/033822 A1

(51) 国际专利分类号:
H04L 9/08 (2006.01)

(21) 国际申请号: PCT/CN2018/088853

(22) 国际申请日: 2018 年 5 月 29 日 (29.05.2018)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201710703108.0 2017年8月16日 (16.08.2017) CN

(71) 申请人: 中国移动通信有限公司研究院 (CHINA MOBILE COMMUNICATION LTD., RESEARCH INSTITUTE) [CN/CN]; 中国北京市西城区宣武门西大街 32 号, Beijing 100053 (CN)。 中国移动通信集团有限公司 (CHINA MOBILE COMMUNICATIONS GROUP CO.,LTD.) [CN/CN]; 中国北京市西城区金融大街29号, Beijing 100032 (CN)。

(72) 发明人: 阎军智 (YAN, Junzhi); 中国北京市西城区金融大街29号, Beijing 100032 (CN)。

(74) 代理人: 北京银龙知识产权代理有限公司(DRAGON INTELLECTUAL PROPERTY LAW FIRM); 中国北京市海淀区西直门北大街32号院枫蓝国际中心2号楼10层, Beijing 100082 (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, 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,

(54) **Title:** METHODS FOR GENERATING AND AUTHENTICATING DIGITAL CERTIFICATE, COMMUNICATION DEVICE, AND STORAGE MEDIUM

(54) **发明名称**: 数字证书的生成、认证方法、通信设备及存储介质

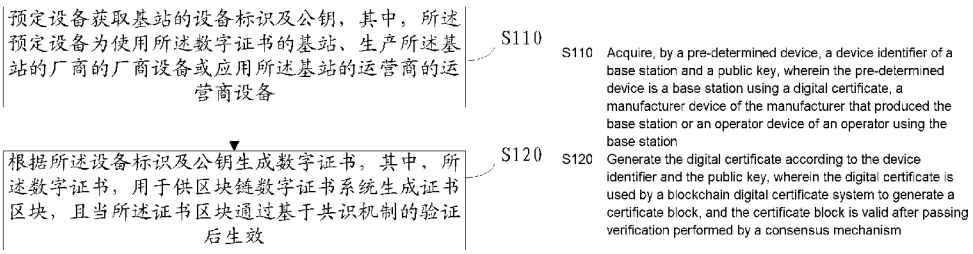

图 1

(57) **Abstract:** Disclosed in an embodiment of the present disclosure are methods for generating and authenticating a digital certificate, a communication device, and a storage medium. The method for generating a digital certificate comprises: acquiring, by a pre-determined device, a device identifier of a base station and a public key, wherein the pre-determined device is a base station using a digital certificate, a manufacturer device of the manufacturer that produced the base station or an operator device of an operator using the base station; and generating the digital certificate according to the device identifier and the public key, wherein the digital certificate is used by a blockchain digital certificate system to generate a certificate block, and the certificate block is valid after passing verification performed by a consensus mechanism.

(57) **摘要**: 本公开实施公开了一种数字证书的生成、认证方法、通信设备及存储介质。本公开实施例提供的数字证书的生成方法，包括：预定设备获取基站的设备标识及公钥，其中，所述预定设备为使用所述数字证书的基站、生产所述基站的厂商的厂商设备或应用所述基站的运营商的运营商设备；根据所述设备标识及公钥生成数字证书，其中，所述数字证书，用于供区块链数字证书系统生成证书区块，且当所述证书区块通过基于共识机制的验证后生效。

WO 2019/033822 A1

[见续页]

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))。

数字证书的生成、认证方法、通信设备及存储介质

相关申请的交叉引用

本申请主张在 2017 年 8 月 16 日在中国提交的中国专利申请号 No. 201710703108.0 的优先权，其全部内容通过引用包含于此。

技术领域

本公开涉及移动通信技术领域，尤其涉及一种数字证书的生成、认证方法、通信设备及存储介质。

背景技术

数字证书就是互联网通讯中标志通讯各方身份信息的一串数字，提供了一种在 Internet 上验证通信实体身份的方式，数字证书不是数字身份证。例如，网关或核心网的网元需要利用安装在基站内的数字证书对基站进行验证。

所述基站可为各种类型的基站，例如，小基站、微基站和家庭基站等。所述家庭基站，又称 HeNB，（Home evolved Node B，家庭演进基站），是一种小型化、低功率蜂窝技术，通过固网宽带接入到移动核心网，为用户设备提供包括传统蜂窝移动通信基础业务在内的固定移动融合业务。

目前 3GPP HeNB 安全规范 TS 33.320 已经定义了 HeNB 的认证方式，HeNB 与安全网关之间采用数字证书进行设备双向认证。为了实现对基站设备的认证，小基站需要配置安装数字证书，该过程需要在接入核心网之前进行，通常有离线申请和在线申请两种方式。

离线申请方式需要设备商首先为小基站产生公私钥对，之后向证书认证（Certificate Authority，CA）机构提供证书生成材料，其中包括小基站的公钥，CA 机构根据申请材料制作并签发证书，设备商获得证书之后需要为小基站配置安装证书。

在线申请方式由小基站发起，首先产生公私钥对，并根据在线证书生成协议生成证书生成请求，发起证书生成流程，CA 机构根据证书生成请求制作并签发证书，小基站接收并安装 CA 签发的证书。

上述离线申请方式，设备商需要向 CA 中心申请数字证书，数字证书由 CA 中心生成，由于不同小基站使用不同的数字证书，个体之间存在较大差异，因此难以在生产线实现批量配置，设备商需要将这些数字证书分别安装到不同的小基站中，需要一台一台进行配置，实施效率较低。

上述在线申请方式，可以采用标准的证书生成协议（例如 CMPv2），也可使用私有的在线申请协议。CMPv2 的问题在于协议复杂，期间需要进行多次签名和验证签名的操作，此外还涉及多个 CA 的互信问题，用于在线申请证书的 CA 需要信任设备上预置的证书，如果存在较多的设备商，CA 需要维护多个根证书列表。

故提升数字证书的配置效率是亟待解决的问题。

发明内容

有鉴于此，本公开实施例期望提供一种数字证书的生成、认证方法、通信设备及存储介质，至少部分解决数字证书的生成效率低的问题。

为达到上述目的，本公开的技术方案是这样实现的：

本公开实施例第一方面提供一种数字证书的生成方法，包括：

预定设备获取基站的设备标识及公钥，其中，所述预定设备为使用所述数字证书的基站、生产所述基站的厂商的厂商设备或应用所述基站的运营商的运营商设备；

根据所述设备标识及公钥生成数字证书，其中，所述数字证书，用于供区块链数字证书系统生成证书区块，且当所述证书区块通过基于共识机制的验证后生效。

基于上述方案，当所述预定设备为所述厂商设备或运营商设备时，所述方法还包括：

将所述数字证书广播到区块链数字证书系统；

当所述证书区块通过验证时，确认所述数字证书生效；

将生效的所述数字证书写入对应的基站。

基于上述方案，所述方法还包括：

当所述预定设备为所述厂商设备或运营商设备时，将生成的数字证书写

入所述基站；其中，所述数字证书，用于所述基站在连接到网络之后自行广播到所述区块链数字证书系统。

基于上述方案，所述预定设备获取基站的设备标识及公钥，包括：

所述基站读取预先存储的所述设备标识；

获取公钥；

所述预定设备生成数字证书，包括：

所述基站根据所述预定信息生成所述数字证书；

所述方法还包括：

将所述数字证书广播到区块链数字证书系统；

当所述证书区块通过验证时，确认所述数字证书生效。

基于上述方案，所述预定设备获取基站的设备标识及公钥，包括：

当所述基站连接到网络后，读取预先存储的所述设备标识；

利用密钥生成算法生成所述公钥。

基于上述方案，所述当所述基站连接到网络后，读取预先存储的所述设备标识，包括：

所述基站在接到网络后并在被设置成接入网网元之前，或被设置成接入网元之后，读取预先存储的所述设备标识；

所述将所述数字证书广播到区块链数字证书系统，包括：

根据预先存储的所述区块链数字证书系统的通信地址，将所述数字证书广播到所述区块链数字证书系统。

本公开实施例第二方面提供一种数字证书的认证方法，应用于网关中，包括：

接收基站发送的认证请求，其中，所述认证请求，用于对所述基站的数字证书进行认证；所述数字证书为所述基站自身生成的或厂商设备生成的；所述厂商设备为所述基站的生产厂商的设备；

基于所述认证请求，查询区块链数字证书系统中存储的所述数字证书的状态信息；

基于所述状态信息认证所述数字证书；

当所述数字证书通过验证时，向所述基站返回认证响应。

基于上述方案，所述接收基站发送的认证请求，包括：

接收携带有所述数字证书的证书标识的认证请求；

所述基于所述认证请求，查询区块链数字证书系统存储的所述数字证书的状态信息，包括：

基于所述证书标识，查询所述区块链数字证书系统中存储的所述数字证书及所述状态信息。

基于上述方案，所述接收基站发送的认证请求，包括：

接收携带有所述数字证书的证书标识及所述数字证书的认证请求。

基于上述方案，所述基于所述认证请求，查询区块链数字证书系统存储的所述数字证书的状态信息，包括：

当所述网关是所述区块链数字证书系统的记账节点时，本地查询所述状态信息；

或者，

当所述网关不是所述区块链数字证书系统的记账节点时，向所述区块链数字证书系统发送所述状态信息。

本公开实施例第三方面提供一种通信设备，其中，所述通信设备为预定设备；所述预定设备为使用所述数字证书的基站、生产所述基站的厂商的厂商设备或应用所述基站的运营商的运营商设备，包括：

获取单元，用于获取基站的设备标识及公钥，其中，

证书生成单元，用于根据所述设备标识及公钥生成数字证书，其中，所述数字证书，用于供区块链数字证书系统生成证书区块，且当所述证书区块通过基于共识机制的验证后生效。

本公开实施例第四方面提供一种通信设备，所述通信设备为网关，包括：

接收单元，用于接收基站发送的认证请求，其中，所述认证请求，用于对所述基站的数字证书进行认证；所述数字证书为所述基站自身生成的或厂商设备生成的；所述厂商设备为所述基站的生产厂商的设备；

查询单元，用于基于所述认证请求，查询区块链数字证书系统中存储的所述数字证书的状态信息；

认证单元，用于基于所述状态信息认证所述数字证书；

发送单元，用于当所述数字证书通过验证时，向所述基站返回认证响应。

本公开实施例第五方面提供一种通信设备，包括：

收发器，用于信息收发；

存储器，用于信息存储；

处理器，分别与所述收发器及存储器连接，用于通过计算机程序的执行控制所述收发器的信息收发、存储器的信息存储，并实现权利要求 1 至 6 任一项提供的数字证书的生成方法，或实现权利要求 7 至 10 任一项提供的数字证书的认证方法。

本公开实施例第六方面提供一种通信设备，包括：收发器、存储器、处理器及存储在存储器上并由处理器执行的计算机程序；

所述处理器分别与所述收发器及所述存储器连接，用于通过所述计算机程序的执行，实现前述一个或多个应用于预定设备中的数字证书的生成方法，或实现前述一个或多个应用于网关中的数字证书的认证方法。

本公开实施例第七方面提供一种计算机存储介质，所述计算机存储介质存储有计算机程序；所述计算机存储被执行后，能够实现前述一个或多个应用于预定设备中的数字证书的生成方法，或实现前述一个或多个应用于网关中的数字证书的认证方法。

本公开实施例的数字证书的生成、认证方法、通信设备及存储介质，数字证书的生成不再是与基站生产商或运营商无关联的第三方机构，例如，CA 生成。所述数字证书可以由基站、厂商设备或运营商设备自行生成，通过减少与 CA 之间的数据交互，减少在 CA 生成数字证书时的排队等待时间，可以加速数字证书的生成，减少数字证书生成所导致的延时，提升了数字证书的生成效率；并且可以实现在基站被配置为接入网网元时或之前，就完整数字证书的生成，具有效率高的特点。

附图说明

图 1 为本公开实施例提供的第一种数字证书的生成方法的流程示意图；

图 2 为本公开实施例提供的第二种数字证书的生成方法的流程示意图；

图 3 为本公开实施例提供的第一种数字证书的认证方法的流程示意图；

图 4 为本公开实施例提供的一种预设设备的结构示意图；

图 5 为本公开实施例提供的一种网关的结构示意图；

图 6 为本公开实施例提供的第一种通信设备的结构示意图；

图 7 为本公开实施例提供的第二种通信设备的结构示意图；

图 8 为本公开实施例提供的第三种数字证书的生成方法的流程示意图；

图 9 为本公开实施例提供的第四种数字证书的生成方法的流程示意图；

图 10 为本公开实施例提供的第二种数字证书的认证方法的流程示意图；

图 11 为本公开实施例提供的第三种数字证书的认证方法的流程示意图。

具体实施方式

以下结合说明书附图及具体实施例对本公开的技术方案做进一步的详细阐述。

如图 1 所示，本实施例提供一种数字证书的生成方法，包括：

步骤 S110：预定设备获取基站的设备标识及公钥，其中，所述预定设备为使用所述数字证书的基站、生产所述基站的厂商的厂商设备或应用所述基站的运营商的运营商设备；

步骤 S120：根据所述设备标识及公钥生成数字证书，其中，所述数字证书，用于供区块链数字证书系统生成证书区块，且当所述证书区块通过基于共识机制的验证后生效。

本实施例提供一种数字证书的生成方法，生成数字证书的设备不再是第三方的 CA 机构，而是需要使用该数字证书的基站自身、生成该基站的厂商的厂商设备，或者应用该基站搭建通信网络的运营商的运营商设备等生产或使用基站等非第三方设备来自行生成数字证书。

在生成数字证书之前，需要获取生成数字证书的所需信息。

在本实施中生成所述数字证书的所需信息包括：基站的设备标识及公钥。在本实施中所述基站的设备标识为全网唯一的标识。

所述设备标识可包括多个序列：厂商设备生成该基站的序列号组成的第一序列、随机产生随机数组成的随机序列及验证该设备标识的验证序列。在一些实施例中，该设备标识可包括：128 个比特或 256 个比特等。其中，形

成设备标识的多个序列，按照一定顺序组成预定比特长度的标识序列。

所述公钥可为利用密钥生成算法生成的公开在网络中的密钥；私钥为与所述公钥对应不对外公开的密钥。通常所述私钥仅存储在所述基站中，所述公钥是公开在网络中。所述公钥和私钥形成密钥对，可以采用非对称加密对基站被配置为接入网元之后的信息交互。在本实施例中所述公钥为生成所述数字证书的依据参数之一。

所述数字证书的内容可包括：

数字证书的版本信息；

数字证书的证书标识，该证书标识可为证书序列号，每个数字证书都有一个唯一的证书序列号，可为生成所述数字证书时向特定设备申请的；而特定设备基于各个设备的申请，统一下发全网唯一的证书序列号；

数字证书所使用的签名算法；

证书的生成机构的机构信息，例如，在本实施例中可为厂商信息。一般机构信息可为机构名称，命名规则一般采用 X.500 格式；

数字证书的有效期，通用的数据字证书一般采用 UTC 时间格式，UTC 的计时范围为 1950-2049；

数字证书所有人的名称，命名规则一般采用 X.500 格式；这里的所有人可为使用该数字证书的基站或基站的厂商。

数值证书所有人的公开密钥，即公钥；

数字证书发行者对数字证书的签名。

在本实施例中所述的数字证书包括的必选内容，可为证书标识、基站的设备标识及公钥等。在一些情况下，所述数字证书还可包括：签名算法及证书有效使用权限等。

所述步骤 S120 具体可包括：利用所述签名算法对所述设备标识及公钥签名处理，并生成包括所述证书标识、公钥及设备标识及签名信息的所述数字证书。在一些实施例中，在本实施例中所述证书标识可为按照预设规则生成的，且通常需要保证每一个数字证书的证书标识是全网唯一的。例如，在本实施例中所述设备标识为全网唯一的标识，则可以基于所述设备标识生成所述证书标识。当然，在一些情况下，所述证书标识也可以是对应的机构预先

颁发给基站的生产厂商的唯一性标识，则这样的话，可以将目前为未使用状态的数字证书分配给对应的数字证书即可。再例如，预设设备还可以在生成数字证书时，向特定设备请求所述数字证书，从而获得所述数字证书。总之，获得所述数字证书的方式有多种，不局限于上述任意一种。

在本实施例中所述数字证书是由使用该证书的基站或生产该基站的厂商生成的，相对于由 CA 生成，不用返回的进行信息交互，提升了数字证书的生成效率，尤其是当 CA 接收到请求很多时导致的配置时延大的问题。

当所述预定设备为所述厂商设备或运营商设备时，所述方法还包括：

将所述数字证书提交如广播到区块链数字证书系统；

当所述证书区块通过验证时，确认所述数字证书生效；

将生效的所述数字证书写入对应的基站。

在本实施例中所述数字证书是利用区块链技术进行生成和存储的。故在本实施例中若生成了一个数字证书，需要将该数字证书广播到区块链数字证书系统中，由区块链数字证书系统中的记账节点基于共识机制进行对应证书区块的验证。仅有包对应数字证书的证书区块通过验证，对应的数字证书才生效。

在本实施例中，所述预定设备为所述厂商设备，厂商设备会连接到区块链数字证书系统，会将生成的数字证书广播到区块链数字证书系统中。

最后当数字证书生效之后，会将生效的数字证书写入到对应的基站中。例如，当前数字证书 A 是基于基站 A 的设备标识生成的，则将生效的数字证书 A 写入到基站 A 中。这样后续，基站被配置为接入网网元之后，就可以直接使用该数字证书 A，或在该数字证书 A 通过认证之后投入使用。

在一些实施例中，生成所述数字证书的设备还是厂商设备，但是厂商设备不与区块链系统连接，不对该数字证书进行生效验证，故在本实施例中，所述方法还包括：

当所述预定设备为所述厂商设备或运营商设备时，将生成的数字证书写入所述基站；其中，所述数字证书，用于所述基站在连接到网络之后自行广播到所述区块链数字证书系统。

厂商设备直接将生成的数字证书写入到基站中，由基站在连接到网络之

后，自行广播到区块链数字证书系统，以使所述数字证书生效。

在一些实施例中，所述预设设备还可以是基站。这时可如图 2 所示，所述步骤 S110 可包括步骤 S111；所述步骤 S111 可包括：

读取预先存储的所述设备标识并获取公钥。所述获取公钥可包括：读取预先存储的公钥，或者，自行利用密钥生成算法生成所述公钥；例如，生成一个随机数，然后利用密钥生成算法分别生成密钥对，从而获得所述公钥。

所述步骤 S120 可包括步骤 S121；所述步骤 S121 可包括：

所述基站根据所述预定信息生成所述数字证书。

所述方法还包括：

步骤 S130：将所述数字证书广播到区块链数字证书系统；

步骤 S140：当所述证书区块通过验证时，确认所述数字证书生效。

在本实施中数字证书是由基站自身生成的，再生成所述数字证书之后，基站会将数字证书广播到区块链数字证书系统，以生效所述数字证书。

具体地，所述步骤 S110 可包括：当所述基站连接到网络后，读取预先存储的所述设备标识；利用密钥生成算法生成所述公钥。

基站不是一开启就启动数字证书的生成路程，而是在基站连接到网络之后，才启动所述数字证书的生成，减少因为数字证书生成早导致的实际投入使用的有效期较短的现象。

在一些实施例中，所述步骤 S110 可包括：

所述基站在接到网络后并在被设置成接入网网元之前，或被设置成接入网元之后，读取预先存储的所述设备标识；

所述步骤 S120 可包括：

根据预先存储的所述区块链数字证书系统的通信地址，将所述数字证书广播到所述区块链数字证书系统。

总之在本实施例中所述基站预先写入了区块链数字证书系统的通信地址，这里的通信地址可以为区块链数字证书系统的网络协议（IP）地址等。一般情况下，所述通信地址可为多个区块链数字证书系统中区块链节点的通信地址，可以以地址表的形式存储在所述基站中。在一些实施例中，所述通信地址也可为一个 IP 地址，例如，可为所述区块链数字证书系统的广播地址等。

在一些情况下，所述基站被安装连接到网络之后，在执行所述基站的初始化配置，以将所述基站配置为接入网网元的过程中，所述基站可以基于预存储的通信地址完成数字证书的生效，这样的话，后续基站被配置完之后，就可以直接使用该生效的数字证书，或者，是直接对该数字证书进行验证了。

当然在另一些情况下，所述基站也可以在完成配置之后，再启动数字证书的生成流程生成所述数字证书。

在本实施例中，所述方法还包括：

在所述数字证书被广播到区块链数字证书系统之前，对所述数字证书进行初次验证。

这里的初次验证可包括以下至少其中之一：

验证所述数字整数的信息格式是否正确；

验证所述数字证书自身的合法性；

验证所述数字证书的证书标识的唯一性；

基于基站即将投入使用的地理位置，验证所述数字证书的地理范围是否在可允许范围内。

总之，在本实施例中为了避免生效有瑕疵的数字证书，在将对应的数字证书广播到数字证书区块链系统之前先进行初次验证，仅有初次验证通过之后，才会对该数据证书进行广播，才会执行生效操作。

如图 3 所示，本实施例提供一种数字证书的认证方法，应用于网关中，包括：

步骤 S210：接收基站发送的认证请求，其中，所述认证请求，用于对所述基站的数字证书进行认证；所述数字证书为所述基站自身生成的或厂商设备生成的；所述厂商设备为所述基站的生产厂商的设备；

步骤 S220：基于所述认证请求，查询区块链数字证书系统中存储的所述数字证书的状态信息；

步骤 S230：基于所述状态信息认证所述数字证书；

步骤 S240：当所述数字证书通过验证时，向所述基站返回认证响应。

本实施例提供的数字证书的认证方法，为应用于基站的安全网关中的方法。

在本实施例中网关需要验证的数字证书首先是基站自行生成的或者是基站的厂商设备生成的。

基站在初始化被配置为接入网网元后，会向网关发起认证请求。该认证请求至少携带有需要认证的数字证书的证书标识。

网关接收到认证请求之后，会通过区块链数字证书系统的对接来认证该数字证书的真实性、可靠性及合法性。具体如，在步骤 S220 中获取所述状态信息，

所述状态信息可包括：指示该数字证书是否存储在区块链数字证书系统的存储状态，若当前验证的数字证书是一个非法证书，则在区块链数字证书系统中就没有该数字证书的存储记录，故可以通过存储状态验证数字证书的合法性和真实性。

所述状态信息还可包括：有效性状态信息；例如，如果发生私钥失密、以及其他可能导致私钥不再安全如果发生私钥失密、以及其他可能导致私钥不再安全的情况，为确保安全，应提前终止证书的有效性，需要将数字证书的状态修改为无效。通过有效性状态信息，可以剔除部分已经无效的数字证书的认证通过。所述状态信息还可包括：完整性状态，例如，在一些伪造的数字证书，可能伪造了合法证书的证书标识；完整性状态可为将基站提交的数字证书传输给区块链数据整数系统，由系统进行全部信息的比对，比对之后获得表征请求认证的数字证书是否完整的状态信息。

总之，本实施例中所述状态信息可为各种状态信息，可为上述状态信息的多种组合，但是不局限于上述任意一种。

在步骤 S230 中基于区块链数字证书系统返回的状态信息，确定是否通过该数字证书的认证。若认证通过则在步骤 S240 中携带有直接或间接指示该数字证书认证通过的信息，若认证未通过，则通过步骤 S240 向基站返回直接或间接指示认证不通过的信息。

在一些实施例中，所述基站若接收到认证不同的认证响应之后，所述数字证书的生成方法，还包括：

删除旧的数字证书；

利用设备标识及公钥重新生成数字证书；

将所述数字证书发送到区块链数字证书系统，以生成证书区块；

当所述证书区块生效后，再将生效的重新生成的数字证书发送给所述网关，请求认证。这样的话，网关会再次收到对重新生成的数字证书进行认证的认证请求，再次执行所述步骤 S210 至步骤 S240。

在一些实施例中，所述步骤 S210 可包括：

接收携带有所述数字证书的证书标识的认证请求；

所述步骤 S220 包括：

基于所述证书标识，查询所述区块链数字证书系统中存储的所述数字证书及所述状态信息。

在本实施例中，所述认证请求仅携带有数字证书的证书标识，但是未携带有数字证书的完整内容。此时，所述步骤 S220 中，网关会同步在区块链数字证书系统中查询数字证书，以获取该基站的数字证书，方便后续利用该数字证书与基站进行通信。

在另一些实施例中，所述步骤 S210 可包括：

接收携带有所述数字证书的证书标识及所述数字证书的认证请求。

此时，所述数字证书已经从基站接收了，则不用在步骤 S220 中再从区块链数字证书系统请求该数字证书了。

在一些实施例中，所述步骤 S220 可包括：当所述网关是所述区块链数字证书系统的记账节点时，本地查询所述状态信息。若网关自身就是区块链数字证书系统的一个记账节点，则该网关可能记录整个区块链数字证书系统中所有的证书区块，则网关可以通过在本地查询证书区块，获取该数字证书的状态信息。

在另一些实施例中，所述步骤 S220 可包括：当所述网关不是所述区块链数字证书系统的记账节点时，向所述区块链数字证书系统发送所述状态信息。

一般这种状态下，所述网关至少记录有区块链数字证书系统的广播地址或多个记账节点的通信地址，网关可以至少通过携带有待认证的数字证书的整数标识的查询请求，接收到区块链数字证书系统返回的数字证书的状态信息。

如图 4 所示，本实施例提供一种通信设备，所述通信设备为预定设备；

所述预定设备为使用所述数字证书的基站、生产所述基站的厂商的厂商设备或应用所述基站的运营商的运营商设备，包括：

获取单元 110，用于获取基站的设备标识及公钥，其中，

证书生成单元 120，用于根据所述设备标识及公钥生成数字证书，其中，所述数字证书，用于供区块链数字证书系统生成证书区块，且当所述证书区块通过基于共识机制的验证后生效。

在本实施例中所述通信设备为基站自身或者为生产所述基站的厂商的通信设备。例如，所述厂商设备可为基站生产厂商的台式电脑或笔记本电脑等设备。

在本实施例中，所述获取单元 110 及证书生成单元 120 可对应于处理器，所述处理器可为中央处理器、微处理器、数字信号处理器、应用处理器、可编程阵列或专用集成电路等。所述处理器可通过计算机程序等计算机可执行代码的执行，实现上述设备标识及公钥的获取，并基于设备标识及公钥为基站生成数字证书。

这样的话，基站的数字证书的生成可以有基站或者基站的生产的厂商自动生成，而不用于 CA 等第三方机构的多次信息交互来生成，大大的提高了数字证书的生成效率。

在一些实施例中，当所述预定设备为所述厂商设备或运营商设备时，所述厂商设备还包括：第一广播单元，对应于网络接口等各种通信接口，用于将所述数字证书广播到区块链数字证书系统；第一确定单元，对应于处理器等具有信息处理的模组，用于当所述证书区块通过验证时，确认所述数字证书生效；第一写入单元，可对应于基站连接的通信接口，可用于将生效的所述数字证书写入对应的基站。

在另一些实施例中，所当所述预定设备为所述厂商设备或运营商设备时，所述厂商设备还包括：

第二写入单元，用于将生成的数字证书写入所述基站；其中，所述数字证书，用于所述基站在连接到网络之后自行广播到所述区块链数字证书系统。

进一步地，所述预定设备可为基站；所述基站可包括：

读取单元，用于读取预先存储的所述设备标识；

公钥获取单元， 用于获取公钥，可包括：读取预先存储的公钥，或者，利用密钥生成算法生成所述公钥；

所述证书生成单元，具体用于根据所述预定信息生成所述数字证书；

所述基站还包括：

第二广播单元，用于将所述数字证书广播到区块链数字证书系统；

生效单元，用于当所述证书区块通过验证时，确认所述数字证书生效。

这里的第二广播单元，同样可对应于通信接口，可用于将生成的数字证书广播发送到区块链数字证书系统。

所述生效单元可对应于接收接口，通过与区块链数字证书系统的信息交互，发现该数字证书所在证书区块基于共识机制通过验证之后，就可认为给数字证书生效了，该数字证书就可以投入使用了。

可选地，所述读取单元，具体可用于当所述基站连接到网络后，读取预先存储的所述设备标识；利用密钥生成算法生成所述公钥。

进一步可选地，所述读取单元，具体用于所述基站在接到网络后并在并被设置成接入网网元之前，或被设置成接入网元之后，读取预先存储的所述设备标识；所述第二广播单元，用于根据预先存储的所述区块链数字证书系统的通信地址，将所述数字证书广播到所述区块链数字证书系统。

如图 5 所示，本实施例提供一种通信设备，所述通信设备为网关，包括：

接收单元 210，用于接收基站发送的认证请求，其中，所述认证请求，用于对所述基站的数字证书进行认证；所述数字证书为所述基站自身生成的或厂商设备生成的；所述厂商设备为所述基站的生产厂商的设备；

查询单元 220，用于基于所述认证请求，查询区块链数字证书系统中存储的所述数字证书及/或所述数字证书的状态信息；

认证单元 230，用于基于所述状态信息认证所述数字证书；

发送单元 240，用于当所述数字证书通过验证时，向所述基站返回认证响应。

本实施例提供的网关可为基站的安全网关。在本实施例中所述基站可为小基站或家庭基站等非宏基站。

在本实施例中所述接收单元 210，可对应于通信接口，可为与基站连接

的网络接口等，可以从基站接收所述认证请求。

在一些实施例中，所述查询单元 220 及认证单元 230，可对应于处理器；所述处理器可为中央处理器、微处理器、数字信号处理器、应用处理器、可编程阵列或专用集成电路等。所述处理器可用于通过计算机程序的执行，可以实现所述状态信息的本地查询及数字证书的认证。

在另一些实施例中，所述查询单元 220 可为通信接口，该通信接口连接到区块链数字证书系统，通过向区块链数字证书系统发送查询请求，并接收区块链数字证书系统基于查询请求返回的至少携带有所述状态信息的查询响应，获得所述状态信息。

所述发送单元 240 可对应于与基站之间的通信接口，可向基站发送认证响应，该认证响应至少携带有指示是否认证通过的信息。

在一些实施例中，所述接收单元 210，具体用于接收携带有所述数字证书的证书标识的认证请求；所述查询单元 220，具体用于基于所述证书标识，查询所述区块链数字证书系统中存储的所述数字证书及所述状态信息。

在另一些实施例中，所述接收单元 210，可用于接收携带有所述数字证书的证书标识及所述数字证书的认证请求。

所述查询单元 220 可本地查询也可以远程查询所述状态信息。例如，所述查询单元 220，可用于当所述网关是所述区块链数字证书系统的记账节点时，本地查询所述状态信息。再例如，所述查询单元 220，还可用于当所述网关不是所述区块链数字证书系统的记账节点时，向所述区块链数字证书系统发送所述状态信息。

如图 6 所示，本实施例提供一种通信设备，该通信设备为基站、生产基站的厂商的厂商设备，或者供基站接入到网络的网关，包括：

收发器 21，用于进行信息收发；

存储器 22，用于信息存储；

处理器 23，分别与所述收发器 21 及存储器 22 连接，用于通过计算机程序的执行，能够控制所述收发器 21 的信息收发及所述存储器 22 的信息存储，并能够前述一个或多个技术方案提供的数字证书的生成方法，或，实现前述一个或多个技术方案提供的数字证书的认证方法。

当所述通信设备为基站自身或厂商设备时，所述处理器 23 可用于实现前述的数字证书的生成方法，例如，可实现图 1 和/或图 2 所示的数字证书的生成方法。

当所述通信设备为网关时，所述处理器 23 可用于实现前述的数字证书的认证方法，至少可以实现如图 3 所示的数字证书的认证方法。

所述收发器 21 可包括：收发天线或网络接口等通信接口。

所述存储器 22 可包括：各种类型的存储介质；所述存储介质可包括：内存及硬盘等存储介质。

所述处理器 23 可以通过集成电路（IIC）总线与所述收发器 21 及存储器 22 连接。

如图 7 所示，本公开实施例还提供一种 UE，包括：收发器 31、存储器 32、处理器 33 及存储在存储器 32 上并由处理器 33 执行的计算机程序 34；

所述处理器 33，分别与所述收发器 31 及存储器 32 连接，用于通过所述计算机程序 34 的执行，能够控制所述收发器的信息收发及所述存储器的信息存储，并能够前述一个或多个技术方案提供的数字证书的生成方法，或，实现前述一个或多个技术方案提供的数字证书的认证方法。

所述收发器 31 可包括：收发天线及网络接口等通信接口。

所述存储器 32 可包括：各种类型的存储介质；所述存储介质可包括：内存及硬盘等存储介质。

所述计算机程序 34 可选为存储所述存储器 32 包括的非瞬间存储介质上。

所述处理器 33 可以通过集成电路（IIC）总线与所述收发器 31 及存储器 32 连接，例如，通过总线读取位于所述计算机程序 34 ，并执行所述计算机程序 34，实现前述一个或多个技术方案提供的获取系统消息异常的处理方法，例如，执行如 1、图 2 及图 3 所示的方法中的一个或多个。

图 6 及图 7 中所示的处理器，均可中央处理器、微处理器、数字信号处理器、应用处理器、可编程阵列或专有集成电路中的任意一种或多种的组合。

本公开实施例一种计算机存储介质，所述计算机存储 介质存储计算机程序；所述计算机程序被执行后，能够并能够实现前述一个或多个技术方案提供的数字证书的生成方法，或，实现前述一个或多个技术方案提供的数字证

书的认证方法。

在本申请提供的与数字证书相关的处理中，包括数字证书的生成及数字证书的认证两方面。以下结合上述任意一个实施例提供几个具体示例：

示例 1：

如图 8 所示，本示例提供一种数字证书生成方法，包括：

步骤 S1：省公司（运营商）或设备商生成小基站的设备标识（ID）、私钥，并生成自签名小基站的数字证书。ID 中包含序列号部分、随机数部分、以及验证部分，确保不与他人重复，且不会被他人产生，区块链证书中包含小基站 ID，从而确保一个小基站对应一个区块链证书。

步骤 S2：省公司或/设备商发起数字证书的上报，将小基站的数字证书上报至区块链数字证书系统。这里的省公司指代的通信运营商对应于一个省的通信设备。

步骤 S3：区块链数字证书系统进行证书签发，具体可包括：验证小基站的数字证书，仅合法的小基站证书能够通过验证。之后区块链证书系统通过共识机制将小基站证书记录到区块链中。一旦数字证书写到区块链中，就意味着数字证书被签发，该数字证书生效，可用于后续认证。其中，在验证小基站证书时，可验证证书自身的合法性，如格式是否正确，ID 是否与其他证书相同，此外还可验证小基站是否在许可范围内，如配置小基站 ID 的黑/白名单，仅在许可范围的小基站证书才能通过验证。

步骤 S4：区块链数字证书系统返回数字证书的签发结果，例如，如果签发失败，那么需要根据失败原因进行相应处理。

步骤 S5：在数字证书生效之后，在小基站的生产线上将小基站的设备标识（ID）、私钥、将该数字证书罐装到小基站。

步骤 S6：若由于重名等原因签发失败则重新执行步骤 S1 至 S5。

在本示例中数字证书可以批量生成并批量进行广播，从而使得数字证书可以批量生效。这样厂商设备或运营商设备可以一次性大批量的生成多个数字证书，并在小基站生产时写入到小基站即可。

示例 2：

本示例区别示例 1 的差异点在于：小基站中不直接存储数字证书，仅存

储公钥及设备标识等信息，所述数字证书的生成包括：

省公司/设备商生成小基站 ID、私钥和公钥，在小基站的生产线上将 ID、私钥、公钥安装至小基站。其中，ID 中包含序列号部分、随机数部分、以及验证部分，确保不与他人重复，且不会被他人产生。

省公司/设备商根据小基站的 ID、私钥和公钥制作自签名证书，证书中包含小基站 ID，从而确保一个小基站对应一个区块链证书。

基站连接到网络之后，自行利用 ID 及公钥生成数字证书，并通过与区块链数字证书系统的交互，广播其自身生成的数字证书，在数字证书被携带基于共识机制验证过后的证书区块之后，生效该数字证书。

如图 9 所示，本示例提供一种数字证书的生成方法，包括：

步骤 S11：小基站在出厂前配置 ID，该 ID 具有一定随机性，同批量数字证书生成部分的描述。

步骤 S12：小基站生成公私钥对，并根据 ID 生成自签名生成数字证书。

步骤 S13：小基站将自己的自签名的数字证书发送给区块链数字证书系统，请求签发证书，即上报数字证书的信息。

步骤 S14：区块链数字证书系统验证小基站提交的数字证书，以签发数字证书，如果验证通过则通过共识机制记录到区块链中。该步骤与示例 1 中提供的方案相同。

步骤 S15：区块链数字证书系统返回证书签发结果。

步骤 S16：若由于重名等原因导致签发失败（即申请失败），则需要根据失败原因进行相应处理，例如，重新执行步骤 S11 至步骤 S15。

示例 3：

本示例提供一种数字证书的认证方法，包括：

安全网关在接收到小基站的数字证书之后，对小基站证书的合法性进行验证，包括：数字证书的证书标识（例如，证书名称）与小基站 ID 是否匹配，数字证书是否处于有效期，之后向区块链数字证书系统查询该数字证书的状态信息，查询请求中包含证书信息，如完整的数字证书或数字证书的散列值。

区块链数字证书系统根据证书信息查找证书最新的状态信息，且将状态信息返回给安全网关。

安全网关根据证书状态对小基站的数字证书进行认证。

该方案中，安全网关可以作为区块链数字证书系统的一部分，例如存储完整的区块链，即可实现对小基站的数字证书的本地查询和认证。

如图 10 所示，本示例提供一种数字证书的认证方法包括：

步骤 S21：小基站启动；

步骤 S22：小基站向安全网关发送初始化请求；

步骤 S23：小基站接收到安全网关的初始化响应；

步骤 S24：小基站向安全网关发送数字证书的认证请求；该认证请求没有携带数字证书的完整内容及携带有证书标识；

步骤 S25：安全网关向区块链数字证书系统发送查询请求；

步骤 S26：区块链数字证书系统查询该数字证书的状态信息；

步骤 S27：区块链数字证书系统向安全网关返回该数字证书的状态信息；

步骤 S28：安全网关基于该状态信息认证小基站的数字证书；

步骤 S29：基于认证通过的数字证书计算得到认证授权字段（IKE-AUTN）；该生成内容会作为认证响应返回给小基站；

步骤 S30：安全网关会向小基站发送认证响应；

步骤 S31：基于认证响应验证网关的数字证书。

示例 4：

如果小基站中未存储自身的数字证书，例如，采用了批量证书生成方案二，那么小基站在与安全网关认证过程中，需要将自身数字证书的 ID 告知安全网关，安全网关向区块链数字证书系统查询响应的数字证书以及证书状态。例如，安全网关在接收到小基站提交的证书标识（CERT_ID）之后，向区块链数字证书系统查询数字证书的状态信息。区块链数字证书系统根据证书信息查找相应证书以及证书状态，并将数字证书及状态返回给安全网关。安全网关根据数字证书及其状态对小基站进行认证。本示例提供的方案，一方面减少了小基站与安全网关之间的通信量，另一方面降低了小基站对证书管理方面的要求，例如证书生成、更新等操作，可降低成本。

具体本示例提供的数字证书的认证方法，可如图 11 所示，包括：

步骤 S41：小基站启动；

步骤 S42：小基站向安全网关发送初始化请求；

步骤 S43：小基站接收到安全网关的初始化响应；

步骤 S44：小基站向安全网关发送数字证书的认证请求；该认证请求携带有数字证书的完整内容及证书标识；

步骤 S45：安全网关向区块链数字证书系统发送查询请求；

步骤 S46：区块链数字证书系统查询该数字证书的状态信息及对应的数字证书；

步骤 S47：区块链数字证书系统向安全网关返回该数字证书的状态信息及数字证书；

步骤 S48：安全网关基于该状态信息认证小基站的数字证书；

步骤 S49：基于认证通过的数字证书计算得到认证授权字段（IKE-AUTN）；该生成内容会作为认证响应返回给小基站；

步骤 S50：安全网关会向小基站发送认证响应；该认证响应中可能还携带有网关的数字证书。

步骤 S51：基于认证响应验证网关的数字证书。

本公开实施例提供的数字证书的生成和认证方法，基站、运营商设备或者设备商自己产生数字证书，无需 CA 机构制作并签发数字证书，从而可以在小基站入网甚至出厂之前进行数字证书配置，可实现批量操作，提高证书生成和配置效率。

在图 10 和图 11 所示的数字证书的认证方法中，虚线框内的部分是改进的通过区块链数字证书系统进行交互，在基站初始化配置时进行数字证书认证的流程。

在一些情况下，可以实现小基站仅存储公钥，不存储数字证书，可以减少小基站与安全网关之间的通信量，还可以降低小基站对数字证书管理方面的要求，降低小基站成本。

利用区块链实现去中心，由于区块链分布式存储数字证书，避免量小基站和安全网关向 CA 机构查询证书状态时产生大量请求。本示例不存在 CA 机构，避免了 CA 建设和维护成本。 对现有方案改动较小，改造成本较低。

在本申请所提供的几个实施例中，应该理解到，所揭露的设备和方法，

可以通过其它的方式实现。以上所描述的设备实施例仅仅是示意性的，例如，所述单元的划分，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，如：多个单元或组件可以结合，或可以集成到另一个系统，或一些特征可以忽略，或不执行。另外，所显示或讨论的各组成部分相互之间的耦合、或直接耦合、或通信连接可以是通过一些接口，设备或单元的间接耦合或通信连接，可以是电性的、机械的或其它形式的。

上述作为分离部件说明的单元可以是、或也可以不是物理上分开的，作为单元显示的部件可以是、或也可以不是物理单元，即可以位于一个地方，也可以分布到多个网络单元上；可以根据实际的需要选择其中的部分或全部单元来实现本实施例方案的目的。

另外，在本公开各实施例中的各功能单元可以全部集成在一个处理模块中，也可以是各单元分别单独作为一个单元，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，也可以采用硬件加软件功能单元的形式实现。

本领域普通技术人员可以理解：实现上述方法实施例的全部或部分步骤可以通过程序指令相关的硬件来完成，前述的程序可以存储于一计算机可读取存储介质中，该程序在执行时，执行包括上述方法实施例的步骤；而前述的存储介质包括：移动存储设备、只读存储器（ROM，Read-Only Memory）、随机存取存储器（RAM，Random Access Memory）、磁碟或者光盘等各种可以存储程序代码的介质。

以上所述，仅为本公开的具体实施方式，但本公开的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本公开揭露的技术范围内，可轻易想到变化或替换，都应涵盖在本公开的保护范围之内。因此，本公开的保护范围应以所述权利要求的保护范围为准。

权 利 要 求 书

1、一种数字证书的生成方法，包括：

预定设备获取基站的设备标识及公钥，其中，所述预定设备为使用所述数字证书的基站、生产所述基站的厂商的厂商设备或应用所述基站的运营商的运营商设备；

根据所述设备标识及公钥生成数字证书，其中，所述数字证书，用于供区块链数字证书系统生成证书区块，且当所述证书区块通过基于共识机制的验证后生效。

2、根据权利要求 1 所述的方法 ，其中，

当所述预定设备为所述厂商设备或运营商设备时，所述方法还包括：

将所述数字证书广播到区块链数字证书系统；

当所述证书区块通过验证时，确认所述数字证书生效；

将生效的所述数字证书写入对应的基站。

3、根据权利要求 1 所述的方法，其中，

所述方法还包括：

当所述预定设备为所述厂商设备或运营商设备时，将生成的数字证书写入所述基站；其中，所述数字证书，用于所述基站在连接到网络之后自行广播到所述区块链数字证书系统。

4、根据权利要求 1 所述的方法，其中，

所述预定设备获取基站的设备标识及公钥，包括：

所述基站读取预先存储的所述设备标识；

获取公钥；

所述预定设备生成数字证书，包括：

所述基站根据所述预定信息生成所述数字证书；

所述方法还包括：

将所述数字证书广播到区块链数字证书系统；

当所述证书区块通过验证时，确认所述数字证书生效。

5、根据权利要求 4 所述的方法，其中，

所述预定设备获取基站的设备标识及公钥，包括：

当所述基站连接到网络后，读取预先存储的所述设备标识；

利用密钥生成算法生成所述公钥。

6、根据权利要求 5 所述的方法 ，其中，

所述当所述基站连接到网络后，读取预先存储的所述设备标识，包括：

所述基站在接到网络后并在被设置成接入网网元之前，或被设置成接入网元之后，读取预先存储的所述设备标识；

所述将所述数字证书广播到区块链数字证书系统，包括：

根据预先存储的所述区块链数字证书系统的通信地址，将所述数字证书广播到所述区块链数字证书系统。

7、一种数字证书的认证方法，应用于网关中，包括：

接收基站发送的认证请求，其中，所述认证请求，用于对所述基站的数字证书进行认证；所述数字证书为所述基站自身生成的或厂商设备生成的；所述厂商设备为所述基站的生产厂商的设备；

基于所述认证请求，查询区块链数字证书系统中存储的所述数字证书的状态信息；

基于所述状态信息认证所述数字证书；

当所述数字证书通过验证时，向所述基站返回认证响应。

8、根据权利要求 7 所述的认证方法，其中，

所述接收基站发送的认证请求，包括：

接收携带有所述数字证书的证书标识的认证请求；

所述基于所述认证请求，查询区块链数字证书系统存储的所述数字证书的状态信息，包括：

基于所述证书标识，查询所述区块链数字证书系统中存储的所述数字证书及所述状态信息。

9、根据权利要求 7 所述的认证方法，其中，

所述接收基站发送的认证请求，包括：

接收携带有所述数字证书的证书标识及所述数字证书的认证请求。

10、根据权利要求 7 至 9 任一项所述的方法，其中，

所述基于所述认证请求，查询区块链数字证书系统存储的所述数字证书的状态信息，包括：

当所述网关是所述区块链数字证书系统的记账节点时，本地查询所述状态信息；

或者，

当所述网关不是所述区块链数字证书系统的记账节点时，向所述区块链数字证书系统查询所述状态信息。

11、一种通信设备，其中，所述通信设备为预定设备；所述预定设备为使用所述数字证书的基站、生产所述基站的厂商的厂商设备或应用所述基站的运营商的运营商设备，包括：

获取单元，用于获取基站的设备标识及公钥，其中，

证书生成单元，用于根据所述设备标识及公钥生成数字证书，其中，所述数字证书，用于供区块链数字证书系统生成证书区块，且当所述证书区块通过基于共识机制的验证后生效。

12、一种通信设备，其中，所述通信设备为网关，包括：

接收单元，用于接收基站发送的认证请求，其中，所述认证请求，用于对所述基站的数字证书进行认证；所述数字证书为所述基站自身生成的或厂商设备生成的；所述厂商设备为所述基站的生产厂商的设备；

查询单元，用于基于所述认证请求，查询区块链数字证书系统中存储的所述数字证书及/或所述数字证书的状态信息；

认证单元，用于基于所述状态信息认证所述数字证书；

发送单元，用于当所述数字证书通过验证时，向所述基站返回认证响应。

13、一种通信设备，包括：

收发器，用于信息收发；

存储器，用于信息存储；

处理器，分别与所述收发器及存储器连接，用于通过计算机程序的执行控制所述收发器的信息收发、存储器的信息存储，并实现权利要求 1 至 6 任一项提供的数字证书的生成方法，或实现权利要求 7 至 10 任一项提供的数字证书的认证方法。

14、一种通信设备，包括：收发器、存储器、处理器及存储在存储器上并由处理器执行的计算机程序；

所述处理器分别与所述收发器及所述存储器连接，用于通过所述计算机程序的执行，实现权利要求 1 至 6 任一项提供的数字证书的生成方法，或实现权利要求 7 至 10 任一项提供的数字证书的认证方法。

15、一种计算机存储介质，所述计算机存储介质存储有计算机程序；所述计算机存储被执行后，能够实现权利要求 1 至 6 任一项提供的数字证书的生成方法，或实现权利要求 7 至 10 任一项提供的数字证书的认证方法。

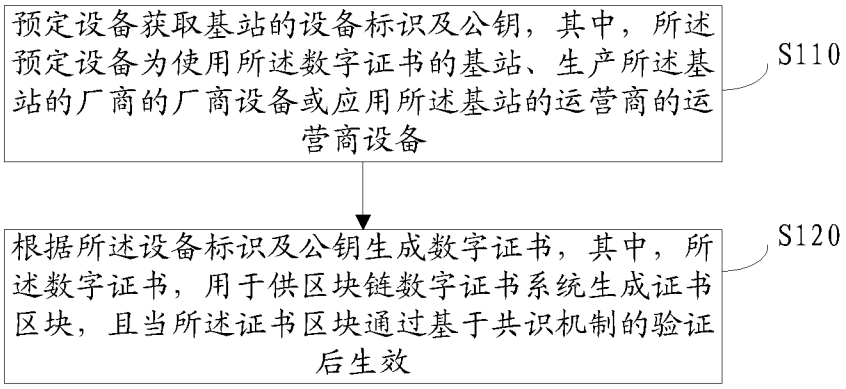
预定设备获取基站的设备标识及公钥，其中，所述预定设备为使用所述数字证书的基站、生产所述基站的厂商的厂商设备或应用所述基站的运营商的运营商设备
S110
根据所述设备标识及公钥生成数字证书，其中，所述数字证书，用于供区块链数字证书系统生成证书区块，且当所述证书区块通过基于共识机制的验证后生效
S120

图 1

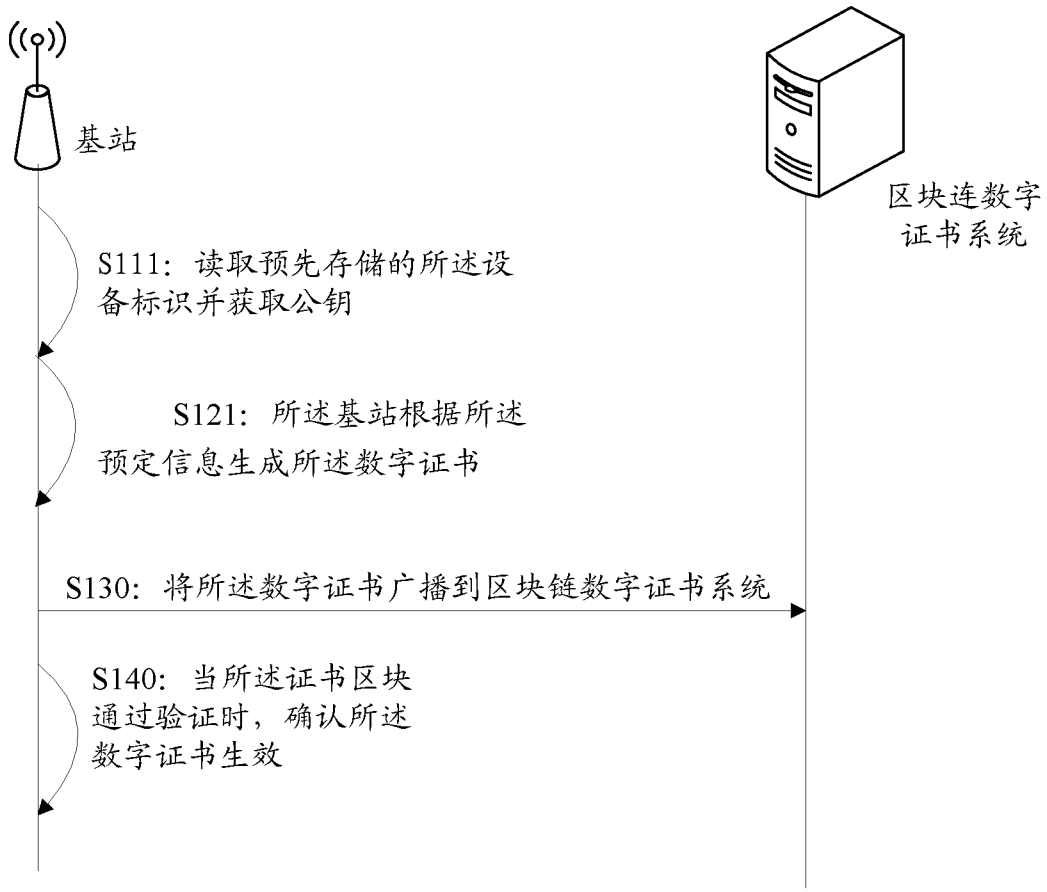
基站
区块连数字证书系统
S111：读取预先存储的所述设备标识并获取公钥
S121：所述基站根据所述预定信息生成所述数字证书
S130：将所述数字证书广播到区块链数字证书系统
S140：当所述证书区块通过验证时，确认所述数字证书生效

图 2

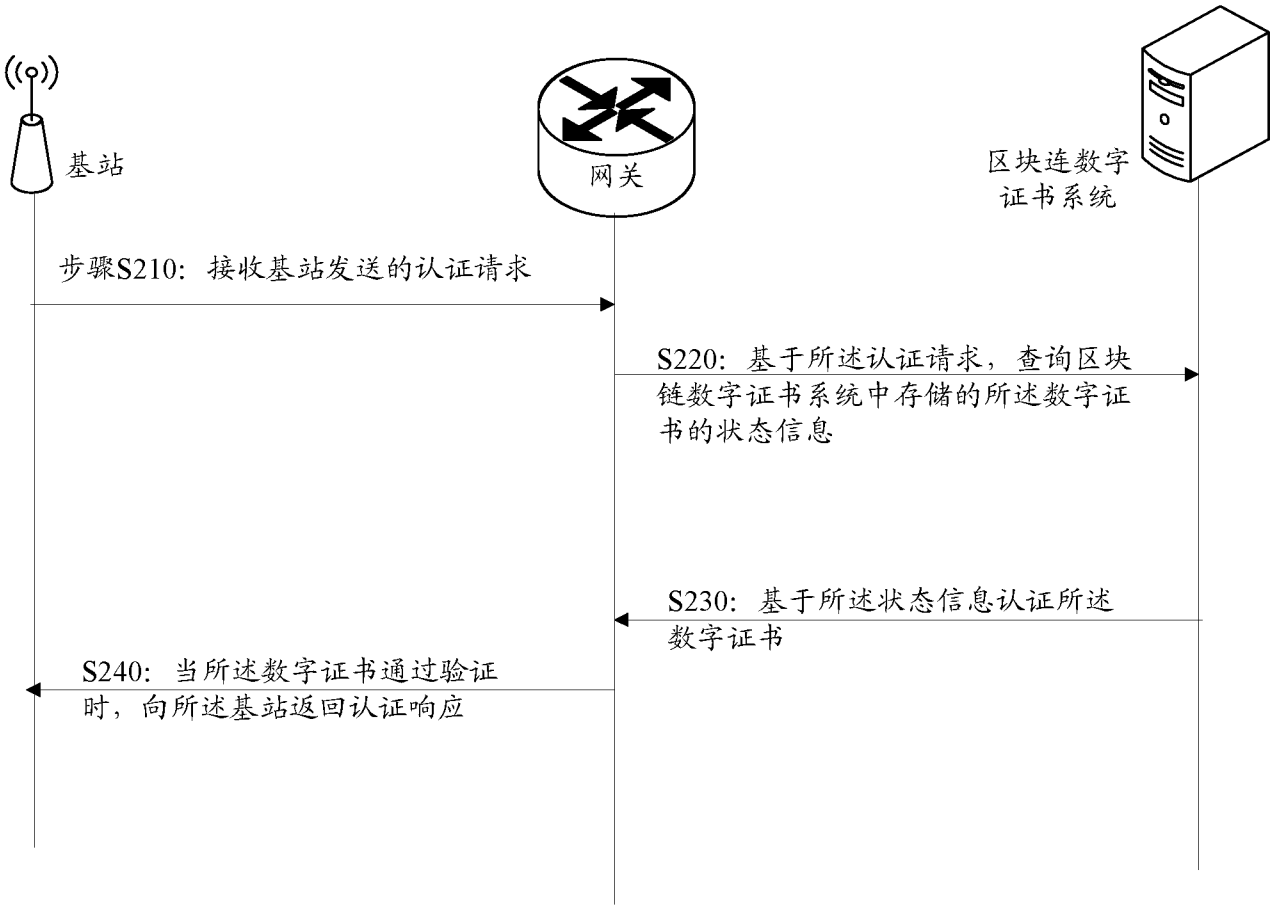
基站
网关
区块连数字证书系统
步骤S210：接收基站发送的认证请求
S220：基于所述认证请求，查询区块链数字证书系统中存储的所述数字证书的状态信息
S230：基于所述状态信息认证所述数字证书
S240：当所述数字证书通过验证时，向所述基站返回认证响应

图 3

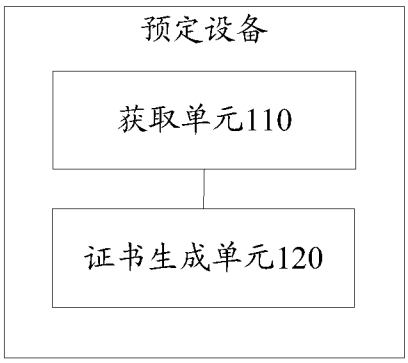
预定设备
获取单元110
证书生成单元120

图 4

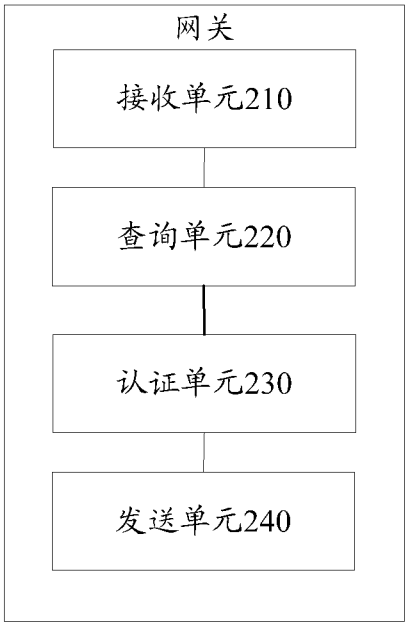
网关
接收单元210
查询单元220
认证单元230
发送单元240

图 5


收发器21
处理器23
存储器22

图 6


收发器31
处理器33
存储器32
计算机程序34

图 7

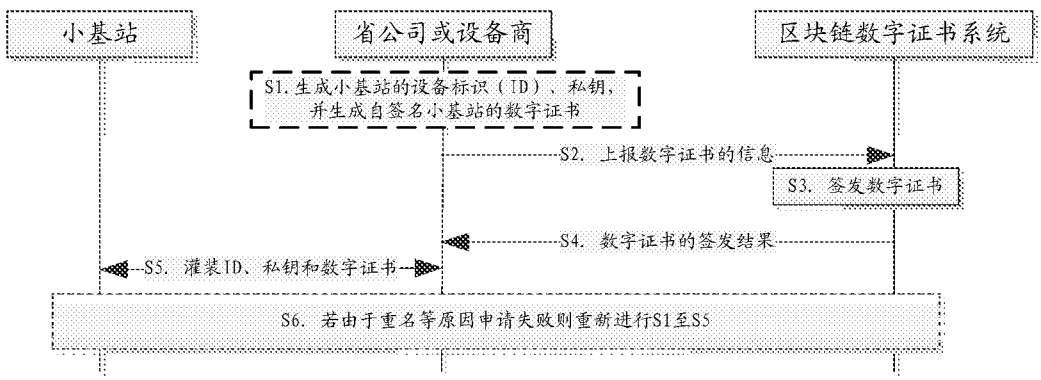
小基站
省公司或设备商
区块链数字证书系统
S1. 生成小基站的设备标识（ID）、私钥，并生成自签名小基站的数字证书
S2. 上报数字证书的信息
S3. 签发数字证书
S4. 数字证书的签发结果
S5. 灌装ID、私钥和数字证书
S6. 若由于重名等原因申请失败则重新进行S1至S5

图 8

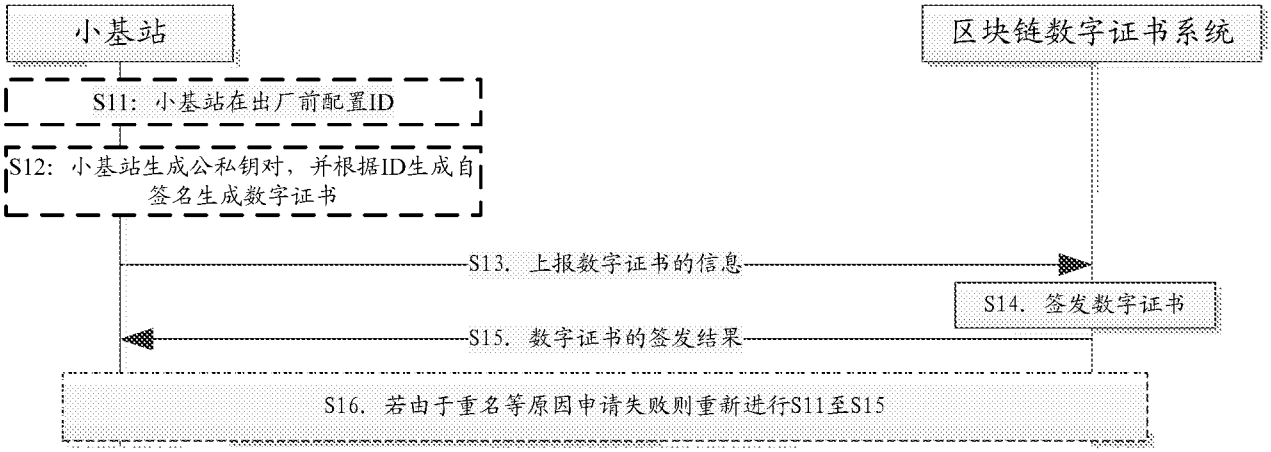
小基站
区块链数字证书系统
S11：小基站在出厂前配置ID
S12：小基站生成公私钥对，并根据ID生成自签名生成数字证书
S13. 上报数字证书的信息
S14. 签发数字证书
S15. 数字证书的签发结果
S16. 若由于重名等原因申请失败则重新进行S11至S15

图 9

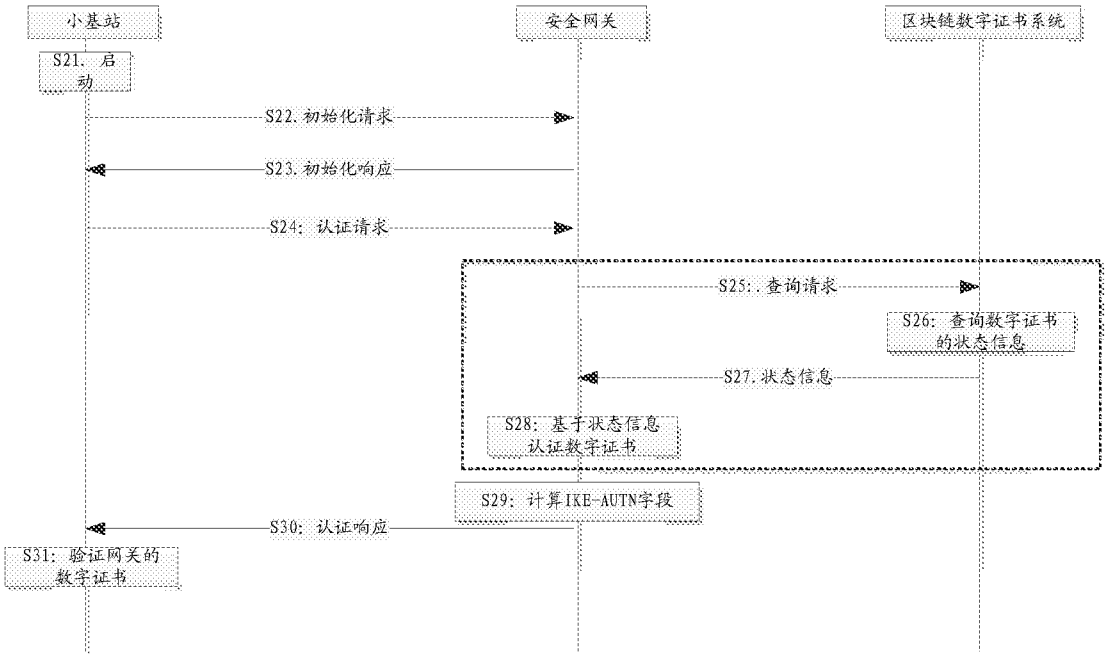
小基站
安全网关
区块链数字证书系统
S21. 启动
S22. 初始化请求
S23. 初始化响应
S24：认证请求
S25：查询请求
S26：查询数字证书的状态信息
S27. 状态信息
S28：基于状态信息认证数字证书
S29：计算IKE-AUTN字段
S30：认证响应
S31：验证网关的数字证书

图 10

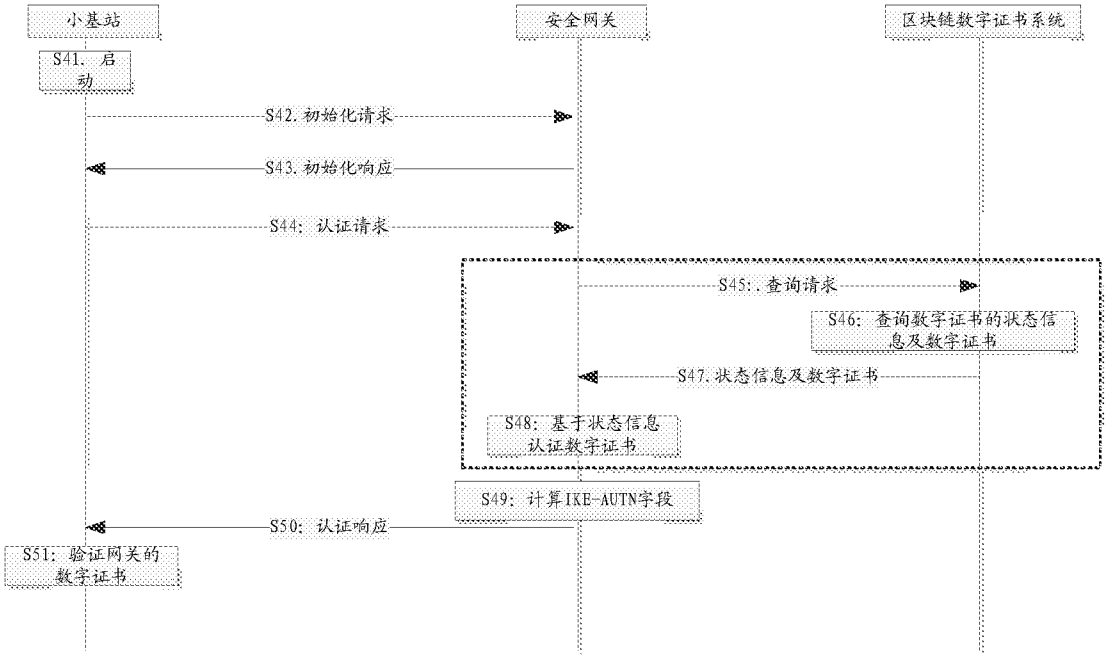
小基站
安全网关
区块链数字证书系统
S41. 启动
S42. 初始化请求
S43. 初始化响应
S44. 认证请求
S45. 查询请求
S46. 查询数字证书的状态信息及数字证书
S47. 状态信息及数字证书
S48. 基于状态信息认证数字证书
S49. 计算IKE-AUTN字段
S50. 认证响应
S51. 验证网关的数字证书

图 11

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2018/088853

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/08(2006.01)i

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)

H04L,G06Q

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)

CPRSABS, SIPOABS, DWPI, USTXT, EPTXT, CNTXT, WOTXT, CNKI, 3GPP: 数字证书, 区块链, 密钥, 公钥, 基站, 没有, 无, 取消, 产生, 生成, 写入, 自己, 自身, 标识, 认证请求, CA, block+, chain+, certificat+, key+, public+, identifier+, ID, base+, station+, nodeB+, eNodeB+, generat+

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 106385315 A (BEIJING SANSEC TECHNOLOGY DEVELOPMENT CO., LTD.) 08 February 2017 (2017-02-08) description, paragraphs 0007-0028	1-6, 11, 13-15
Y	CN 106385315 A (BEIJING SANSEC TECHNOLOGY DEVELOPMENT CO., LTD.) 08 February 2017 (2017-02-08) description, paragraphs 0007-0028	7-10, 12
Y	CN 105472604 A (ZTE CORPORATION) 06 April 2016 (2016-04-06) claim 4	7-10, 12
A	CN 106789041 A (JIANGSU XINYUAN JIUAN INFORMATION TECHNOLOGY CO., LTD.) 31 May 2017 (2017-05-31) entire document	1-15
A	US 2016330035 A1 (SHOCARD, INC.) 10 November 2016 (2016-11-10) entire document	1-15
A	WO 2017065389 A1 (COINPLUG INC.) 20 April 2017 (2017-04-20) entire document	1-15

☐ 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	Date of mailing of the international search report
13 August 2018	**05 September 2018**

Name and mailing address of the ISA/CN	Authorized officer
State Intellectual Property Office of the P. R. China **No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088** **China**	
Facsimile No. **(86-10)62019451**	Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2018/088853

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 106385315 A	08 February 2017	None	
CN 105472604 A	06 April 2016	WO 2015154555 A1	15 October 2015
CN 106789041 A	31 May 2017	None	
US 2016330035 A1	10 November 2016	US 9876646 B2	23 January 2018
WO 2017065389 A1	20 April 2017	KR 101637854 B1	08 July 2016

国际检索报告

国际申请号
PCT/CN2018/088853

A. 主题的分类

H04L 9/08(2006.01)i

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)

H04L,G06Q

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））

CPRSABS，SIPOABS，DWPI，USTXT，EPTXT，CNTXT，WOTXT，CNKI，3GPP: 数字证书，区块链，密钥，公钥，基站，没有，无，取消， 产生，生成，写入，自己，自身，标识，认证请求，CA，block+， chain+， certificat+， key+， public+， identifier+， ID， base+， station+， nodeB+， eNodeB+， generat+

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
X	CN 106385315 A (北京三未信安科技发展有限公司) 2017年 2月 8日 (2017-02-08) 说明书第0007-0028段	1-6，11，13-15
Y	CN 106385315 A (北京三未信安科技发展有限公司) 2017年 2月 8日 (2017-02-08) 说明书第0007-0028段	7-10，12
Y	CN 105472604 A (中兴通讯股份有限公司) 2016年 4月 6日 (2016-04-06) 权利要求4	7-10，12
A	CN 106789041 A (江苏信源久安信息科技有限公司) 2017年 5月 31日 (2017-05-31) 全文	1-15
A	US 2016330035 A1 (识卡公司) 2016年 11月 10日 (2016-11-10) 全文	1-15
A	WO 2017065389 A1 (COINPLUG INC) 2017年 4月 20日 (2017-04-20) 全文	1-15

☐ 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	国际检索报告邮寄日期
2018年 8月 13日	2018年 9月 5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 传真号 (86-10)62019451	受权官员 刘琼艳 电话号码 86-010-62088431

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2018/088853

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	106385315	A	2017年 2月 8日		无		
CN	105472604	A	2016年 4月 6日	WO	2015154555	A1	2015年 10月 15日
CN	106789041	A	2017年 5月 31日		无		
US	2016330035	A1	2016年 11月 10日	US	9876646	B2	2018年 1月 23日
WO	2017065389	A1	2017年 4月 20日	KR	101637854	B1	2016年 7月 8日