

(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
2018 年 10 月 4 日 (04.10.2018)



(10) 国际公布号
WO 2018/177143 A1

(51) 国际专利分类号:
H04L 12/28 (2006.01)

(21) 国际申请号: PCT/CN2018/079283

(22) 国际申请日: 2018 年 3 月 16 日 (16.03.2018)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201710211600.6 2017年3月31日 (31.03.2017) CN

(71) 申请人: 华为技术有限公司 (HUAWEI TECHNOLOGIES CO., LTD.) [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(72) 发明人: 朱成康(CHU, Chengkang); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 时杰(SHI, Jie); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 方成方(FANG, Chengfang); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 方习文(FANG, Xiwen); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(74) 代理人: 深圳市深佳知识产权代理事务所(普通合伙)(SHENPAT INTELLECTUAL PROPERTY AGENCY); 中国广东省深圳市国贸大厦15楼西座1521室, Guangdong 518014 (CN)。

(54) Title: IDENTITY AUTHENTICATION METHOD AND SYSTEM, SERVER AND TERMINAL

(54) 发明名称: 一种身份认证的方法、系统及服务器和终端

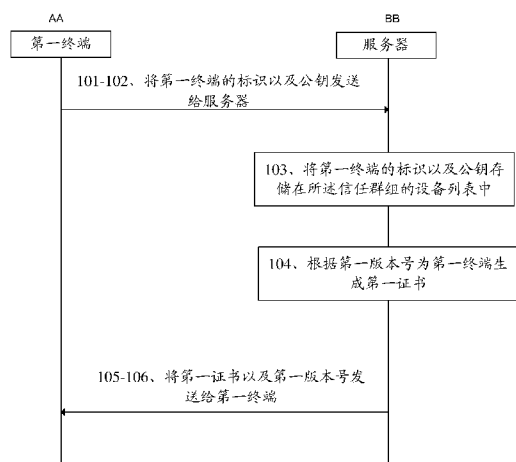


图 2

101-102 Transmit the identifier of a first terminal and a public key to a server
103 Store the identifier of the first terminal and the public key in a device list of a trust group
104 Generate a first certificate for the first terminal according to a first version number
105-106 Send the first certificate and the first version number to the first terminal
AA First terminal
BB Server

(57) Abstract: Disclosed in the embodiments of the present application is an identity authentication method, comprising: when a server receives a group joining request for joining a trust group which is sent by a first terminal, the server generates a first certificate for the first terminal according to a first version number, and the server sends the first certificate and the first version number to the first terminal; and when the server confirms that a second terminal is revoked from the trust group, the server updates the first version number to a second version number according to a preset rule, the server generates corresponding second certificates for the terminals not revoked from the trust group respectively according to the second version number, and the server sends the corresponding second certificates and second version numbers to the terminals not revoked from the trust group respectively. Hence, a terminal, when carrying out authentication, may carry out identity authentication by means of comparing the version number of a counter part, thus increasing the efficiency of authentication.

(57) 摘要: 本申请实施例公开了一种身份认证的方法, 包括: 当服务器接收第一终端发送的加入信任群组的入群请求时, 服务器根据第一版本号为第一终端生成第一证书, 服务器向第一终端发送第一证书以及第一版本号; 当服务器确认第二终端从信任群组中撤销时, 服务器按照预设规则更新第一版本号为第二版本号, 服务器根据第二版本号为信任群组中未撤销的终端分别生成对应的第二证书, 服务器向信任群组中未撤销的终端分别发送对应的第二证书以及第二版本号。这样, 使得终端在进行认证时, 可以通过对比对方的版本号, 则可以进行身份验证, 提高了验证的效率。

(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, 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))。

—1—

一种身份认证的方法、系统及服务器和终端

本申请要求于 2017 年 3 月 31 日提交中国专利局、申请号为 201710211600.6、发明名称为“一种身份认证的方法、系统及服务器和终端”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**

本申请涉及认证领域，尤其是一种身份认证的方法、系统及服务器和终端。

背景技术

在未来物联网的场景下，所有设备皆以各种方式连接上网，但设备间常常需要成为一个群组，共同协作，例如在一个智慧家庭内，家里的冰箱、电视、洗衣机、空调、灯、智能锁、网关、手机、平板等都要能互相通信，让主人能够简单地控制各个设备，以及让设备间自行沟通，例如一打开智能门锁，锁即发出指令将屋内的电灯及空调打开；当衣服洗好时，洗衣机在电视上提醒主人可以晒干等等。诸如此类的设备间通信，若没有适当的安全保护，极有可能成为黑客攻击的目标。

设备间通信的安全保护不外乎两方面，认证与加密。认证指的是两个设备间要彼此通信之前，必须先确认对方是我们要沟通的可信任目标，而不是黑客伪造的设备。而加密则是开始通信后，对传输的信息作加密保护，避免黑客从中窃听。一般设备经过认证之后，可以通过密钥交换协议来交换密钥并加密，因此主要的安全关键还是在设备的认证。建立一个信任群组，首先需要有一个信任中心，负责签发每个设备的公钥证书，也就是设备的身份证，内含信任中心对设备公钥的签名，设备内则握有相对应的私钥。公钥证书是公开信息，当设备要证明自己的身份时，必须提出公钥证书，并以相对应的私钥来签名，证明拥有此证书对应的私钥。因此，设备认证最重要的就是密钥管理，如何正确的让每个设备确认其他设备的公钥证书还在信任群组内而没有被注销，是一个重要的课题。

目前互联网上面最普遍的公钥基础设施（英文全称：Public Key Infrastructure，英文缩写：PKI）架构是建立一个证书管理机构（英文全称：Certificate Authority，英文缩写：CA）作为可信中心，由此 CA 签发每个设备的公钥证书。每当有设备要加入群组时，就和 CA 申请公钥证书，当有群组成员需要被撤销时，则 CA 将此设备放入一个撤销列表。两设备要做认证时，验证方收到对方公钥证书后，先向 CA 索取撤销列表，并使用 CA 的公钥去验证证书和撤销列表的签名是否正确。若签名都正确，且此证书不在撤销列表内，则认证成功，可基于此公钥进行密钥交换。这样，每次基于对方公钥进行密钥交换，通信成本大，回合数多，且无法做到预计算，使得认证的效率比较低。

发明内容

本申请实施例提供了一种身份认证的方法、系统及服务器和终端，用于提高认证的效率。

本申请实施例第一方面提供一种身份认证的方法，包括：

35 当第一终端加入信任群组时，服务器接收到第一终端的入群请求，该入群请求包含第一终端的标识和公钥，服务器将第一终端的标识和公钥存储于设备列表中，并通过服务器的私钥根据第一版本号为第一终端生成第一证书，生成第一证书的条件参数还可以包括第

-2-

一终端的标识、公钥、该信任群组名称标识，服务器向第一终端发送所述第一证书以及第一版本号；其中，设备列表中存储该信任群组中的所有终端的标识和公钥。

当服务器确认第二终端从信任群组中撤销时，服务器将该第二终端的标识和公钥从设备列表中删除，并且服务器按照预设规则更新所述第一版本号为第二版本号，比如版本号可以是一个数值，该预设规则可以是累加规则，若第一版本号为数值 10，那么累加一次得到第二版本号为数值 11；服务器根据第二版本号为所述信任群组中未撤销的终端分别生成对应的第二证书，生成第二证书的条件参数还可以包括所对应的终端的标识、公钥、该信任群组名称标识；生成第二证书后，服务器向所述信任群组中未撤销的终端分别发送对应的第二证书以及第二版本号。其中，第一终端与第二终端可以为同一终端，也可以为不同的终端。

这样，在每次有终端从信任群组中撤销时，服务器均会更新一次版本号，并重新生成证书，将更新后的版本号和新生成的证书发送给未撤销的终端，使得未撤销的终端的版本号相同，而已经被撤销的终端的版本号为旧的版本号，与未撤销的终端的版本号不同。这样，在终端在进行认证时，可以通过对比对方的版本号，则可以进行身份验证，提高了验证的效率。

一种可能的实现方式中，服务器还可以将设备列表发送给第一终端，以使得第一终端进行存储该设备列表，该设备列表包含信任群组中所有未撤销的终端的标识以及公钥，这样，第一终端在认证过程中则可以从设备列表中获取待认证终端的公钥从而进行认证处理。比如，在第一终端认证第二终端时，第一终端在确认第二终端的版本号与自己所存储的版本号相同时，第一终端则可以通过设备列表中第二终端的公钥进行数据包的加密处理，从而与第二终端进行通信认证。或者，第一终端可以直接查找设备列表中是否有第二终端的公钥，则可以直接通过第二终端的公钥进行加密数据包，进行通信认证。

另一种可能的实现方式中，服务器还可以向所述信任群组中所有未撤销的终端发送存储有新增的第一终端的标识以及公钥的设备列表。同样，用于终端在认证过程中可以通过设备列表中获取待认证的终端的公钥进行认证处理。

本申请实施例第二方面提供一种身份认证的方法，包括：

当第一终端加入信任群组时，第一终端向服务器发送请求加入信任群组的入群请求，该入群请求包含第一终端的标识和公钥；第一终端接收服务器发送的第一证书以及第一版本号，其中第一证书为服务器根据所述第一版本号为第一终端所生成的证书；

当第二终端从信任群组中撤销时，第一终端接收服务器发送的第二证书以及第二版本号，其中，第二版本号为服务器按照预设规则所更新的版本号，第二证书为服务器根据第二版本号为第一终端所生成的证书。

一种可能的实现方式中，该方法还包括：

第一终端接收服务器发送的设备列表，其中，设备列表包含信任群组中所有未撤销的终端的标识以及公钥，以使得用于第一终端在认证过程中从设备列表中获取待认证终端的公钥从而进行认证处理。

本申请实施例第三方面提供一种身份认证的方法，包括：

—3—

第一终端接收第二终端发送的包含第一版本号和第二终端的标识的认证请求，其中，第一版本号为服务器发送给第一终端的版本号，当有终端从信任群组中撤销时，服务器会对版本号进行累加，并将累加后的版本号发送给信任群组中所有未撤销的终端；

第一终端判断第一版本号是否小于第二版本号，其中，第二版本号为第一终端所存储的服务器所发送的版本号；

当第一终端确定第一版本号小于第二版本号时，第一终端确定第二终端的身份失效。

这样，在认证过程中，第一终端只需获取第二终端的标识和版本号，通过对比第二终端的版本号与自己所存储的版本号的大小，则可以判断第二终端的版本号是否是旧的版本号，若是旧的版本号，则标识第二终端已经被服务器所撤销，则确定第二终端的身份失效，这样，不仅实现了离线认证，并且认证过程中认证信息简单，信令交互较少，提高了认证的效率。

一种可能的实现方式中，第一终端存储有服务器发送的设备列表，设备列表中包含信任群组中所有未撤销的终端的记录信息，该记录信息可以包括信任群组中未撤销的终端的标识和公钥，以及每个标识和公钥的对应关系；

当第一终端确定第一版本号小于或等于第二版本号时，第一终端判断设备列表中是否包含第二终端的记录信息；第一终端可以通过将接收到的第二终端发送的标识对设备列表中的记录信息进行匹配，若存在匹配相同的结果，则表示设备列表中包含第二终端的记录信息，若不存匹配相同的结果，则表示设备列表中不包含第二终端的记录信息；

当第一终端确定设备列表中不包含第二终端的记录信息时，第一终端确定第二终端的身份失效。

在实际应用中，由于网络覆盖的原因，服务器在更新了版本号和证书后，有的终端并不能及时更新版本号和证书，因此版本号其实是旧的版本号，但是若第一终端保存了服务器发送的设备列表，而第一终端的版本号是更新后的版本号，那么第一终端可以从设备列表终端判断该第二终端是否已经被撤销，若该设备列表中仍包含第二终端的标识和公钥，则标识该第二终端未被服务器撤销。若该设备列表中已经不包含该第二终端的标识和公钥了，那么标识第二终端已经被撤销，则确定第二终端的身份失效。这样，对于未能及时更新版本号和证书的未被撤销的终端，也能够实现认证，提高了认证的准确性。

另一种可能的实现方式中，第一终端存储有服务器发送的设备列表，设备列表中包含信任群组中所有未撤销的终端的标识和公钥；

当第一终端确定第一版本号大于第二版本号时，第一终端接收第二终端发送的第二证书；

第一终端根据服务器的公钥验证第二证书是否为服务器发送给第二终端的证书；

当第一终端确定第二证书不为服务器发送给第二终端的证书时，第一终端确定第二终端的身份失效。

若第二终端的版本号比第一终端的版本号大，那么存在两种可能，第一种可能是第二终端更新了版本号和证书，而第一终端未更新版本号和证书；第二种可能是第二终端恶意修改了一个较大的版本号，从而希望得到第一终端的认证成功。此时，第一终端无法判断

—4—

是何种情况，因此，第一终端需要第二终端发送证书给第一终端，第一终端通过服务器的公钥来验证该证书是否是服务器生成的，若是，则表示为上述的第一种可能，若否，则表示为上述的第二种可能，此时则确定第二终端的身份失效。这样，对于自身未及时更新版本号 and 证书的情况以及待认证终端恶意修改版本号的情况，均能准确判断并认证，提高了认证的准确性。

本申请实施例第四方面提供一种身份认证的方法，所述方法包括：

第一终端接收第二终端发送的认证请求，所述认证请求包含第一版本号 and 所述第二终端的标识，所述第一版本号为服务器发送给所述第一终端的版本号，当有终端从信任群组中撤销时，服务器会对版本号进行累减，并将累减后的版本号发送给所述信任群组中所有未撤销的终端；

所述第一终端判断所述第一版本号是否大于第二版本号，其中，所述第二版本号为所述第一终端所存储的服务器所发送的版本号；

当所述第一终端确定所述第一版本号大于所述第二版本号时，所述第一终端确定所述第二终端的身份失效。

一种可能的实现方式中，所述第一终端存储有所述服务器发送的设备列表，所述设备列表中包含所述信任群组中所有未撤销的终端的记录信息，该记录信息包括信任群组中未撤销的终端的标识和公钥，以及每个标识和公钥的对应关系；

当所述第一终端确定所述第一版本号大于或等于所述第二版本号时，所述方法还包括：

所述第一终端判断所述设备列表中是否包含所述第二终端的记录信息；第一终端可以通过将接收到的第二终端发送的标识对设备列表中的记录信息进行匹配，若存在匹配相同的结果，则表示设备列表中包含第二终端的记录信息，若不存匹配相同的结果，则表示设备列表中不包含第二终端的记录信息；

当所述第一终端确定所述设备列表中不包含所述第二终端的记录信息时，所述第一终端确定所述第二终端的身份失效。

另一种可能的实现方式中，所述第一终端存储有所述服务器发送的设备列表，所述设备列表中包含所述信任群组中所有未撤销的终端的标识和公钥；

当所述第一终端确定所述第一版本号小于所述第二版本号时，所述方法还包括：

所述第一终端接收所述第二终端发送的第二证书；

所述第一终端根据所述服务器的公钥验证所述第二证书是否为所述服务器发送给第二终端的证书；

当所述第一终端确定所述第二证书不为所述服务器发送给第二终端的证书时，所述第一终端确定所述第二终端的身份失效。

本申请实施例第五方面提供一种服务器，该服务器包括：

生成单元，用于当接收第一终端发送的加入信任群组的入群请求时，根据第一版本号为第一终端生成第一证书；

发送单元，用于向第一终端发送第一证书以及第一版本号；

—5—

更新单元，用于当确认第二终端从信任群组中撤销时，服务器按照预设规则更新第一版本号为第二版本号；

生成单元还用于，根据第二版本号为信任群组中未撤销的终端分别生成对应的第二证书；

5 发送单元还用于，向信任群组中未撤销的终端分别发送对应的第二证书以及第二版本号。

本申请实施例第六方面提供一种终端，当终端为第一终端时，终端包括：

发送单元，用于向服务器发送加入信任群组的入群请求，入群请求包含第一终端的标识和公钥；

10 接收单元，用于接收服务器发送的第一证书以及第一版本号，其中第一证书为服务器根据第一版本号为第一终端所生成的证书；

接收单元还用于，当第二终端从信任群组中撤销时，接收服务器发送的第二证书以及第二版本号，其中，第二版本号为服务器按照预设规则所更新的版本号，第二证书为服务器根据第二版本号为第一终端所生成的证书。

15 本申请实施例第七方面提供一种终端，当终端为第一终端时，终端包括：

接收单元，用于接收第二终端发送的认证请求，认证请求包含第一版本号和第二终端的标识，第一版本号为服务器发送给第一终端的版本号，当有终端从信任群组中撤销时，服务器会对版本号进行累加，并将累加后的版本号发送给信任群组中所有未撤销的终端；

20 判断单元，用于判断第一版本号是否小于第二版本号，其中，第二版本号为第一终端所存储的服务器所发送的版本号；

确定单元，用于当确定第一版本号小于第二版本号时，第一终端确定第二终端的身份失效。

本申请实施例第八方面提供一种终端，当终端为第一终端时，终端包括：

25 第一终端接收第二终端发送的认证请求，所述认证请求包含第一版本号和所述第二终端的标识，所述第一版本号为服务器发送给所述第一终端的版本号，当有终端从信任群组中撤销时，服务器会对版本号进行累减，并将累减后的版本号发送给所述信任群组中所有未撤销的终端；

所述第一终端判断所述第一版本号是否大于第二版本号，其中，所述第二版本号为所述第一终端所存储的服务器所发送的版本号；

30 当所述第一终端确定所述第一版本号大于所述第二版本号时，所述第一终端确定所述第二终端的身份失效。

本申请实施例第九方面提供一种身份认证的系统，包括：服务器、第一终端以及第二终端；

第一终端用于，向服务器发送加入信任群组的入群请求；

35 服务器用于，根据第一版本号为第一终端生成第一证书；

服务器还用于，向第一终端发送第一证书以及第一版本号；

第一终端还用于，接收服务器发送的第一证书以及第一版本号；

—6—

当服务器确认第二终端从信任群组中撤销时，服务器还用于，按照预设规则更新第一版本号为第二版本号；

服务器还用于，根据第二版本号为信任群组中未撤销的终端分别生成对应的第二证书；

5 服务器还用于，向信任群组中未撤销的终端分别发送对应的第二证书以及第二版本号；

第一终端还用于，接收服务器发送的第二证书以及第二版本号。

10 本申请实施例第十方面提供一种服务器，包括：处理器、存储器、收发器，处理器、存储器以及收发器通过总线连接，存储器存储有计算机指令，处理器通过执行所述计算机指令用于实现如第一方面所提供的身份认证的方法。

本申请实施例第十一方面提供一种终端，包括：处理器、存储器、收发器，处理器、存储器以及收发器通过总线连接，存储器存储有计算机指令，处理器通过执行所述计算机指令用于实现第二方面至第四方面所提供的身份认证的方法。

15 本申请实施例第十二方面提供一种存储介质，该存储介质存储有用于实现第一方面至第四方面中身份认证的方法的计算机指令。

本申请实施例第十三方面提供了一种计算机程序产品，该计算机程序产品包括计算机软件指令，该计算机软件指令可通过处理器进行加载来实现上述第一方面至第四方面任意一种实现方式的身份认证的方法中的流程。

从以上技术方案可以看出，本申请实施例具有以下优点：

20 当服务器接收第一终端的请求加入信任群组的入群请求时，服务器根据第一版本号为第一终端生成第一证书，服务器向第一终端发送第一证书以及第一版本号，当服务器确认第二终端从信任群组中撤销时，服务器按照预设规则更新第一版本号为第二版本号，服务器根据第二版本号为信任群组中未撤销的终端分别生成对应的第二证书，服务器向信任群组中未撤销的终端分别发送对应的第二证书以及第二版本号。这样，使得终端在进行认证
25 时，可以通过对比对方的版本号，则可以进行身份验证，提高了验证的效率。

附图说明

图1为本申请实施例中身份认证的方法所应用的一个系统架构示意图；

图2为本申请实施例中身份认证的方法的一个实施例示意图；

图3为本申请实施例中身份认证的方法的另一个实施例示意图；

30 图4为本申请实施例中身份认证的方法的另一个实施例示意图；

图5为本申请实施例中身份认证的方法的另一个实施例示意图；

图6为本申请实施例中身份认证的方法的另一个实施例示意图；

图7为本申请实施例中服务器的一个实施例示意图；

图8为本申请实施例中终端的一个实施例示意图；

35 图9为本申请实施例中终端的另一个实施例示意图；

图10为本申请实施例中服务器的另一个实施例示意图；

图11为本申请实施例中终端的另一个实施例示意图；

图 12 为本申请实施例中身份认证的系统的一个实施例示意图。

具体实施方式

本申请实施例提供了一种身份认证的方法、系统及服务器和终端，用于提高认证的效率。

参照图 1 所示，图 1 为本申请实施例中身份认证的方法所应用的一个系统架构示意图。

在该架构中，包含了主人终端、访客终端、智能终端以及家庭网关，其中，家庭网关分别与主人终端、访客终端、以及智能终端通过有线或者无线连接。家庭网关用作服务功能，即家庭网关是一种服务器。主人终端具备比其它终端更多的功能权限，比如通知家庭网关允许某终端加入信任群组，或者发送指令给家庭网关对某终端从信任群组中撤销等。家庭网关建立一个信任群组，家庭网关作为该信任群组的信任中心，负责签发每个终端设备的公钥证书，也就是终端设备的身份证，内含信任中心对终端设备公钥的签名，终端设备内则握有相对应的私钥。公钥证书是公开信息，当终端设备要证明自己的身份时，必须提出公钥证书，并以相对应的私钥来签名，证明拥有此证书对应的私钥。

在本申请实施例中，提出一种信任群组基于计数器的认证与密钥管理机制，通过简单高效的一个计数器，能够更有效率地进行认证以及管理群组密钥。具体的，家庭网关维护一个信任群组的设备列表以及一个版本号，该设备列表中存储有该信任群组中所有终端的标识和公钥，以及终端的标识和公钥的对应关系。当与新的终端要加入信任群组时，家庭网关需要获取该新终端的标识和公钥，并将该终端的标识和公钥加入至该设备列表中，并存储该新终端的标识和公钥的对应关系。同时，家庭网关需要将当前所维护的版本号发送给新加入的终端，使得当前所有的位于该信任群组内的终端所接收到的版本号一致。当有终端需要从信任群组中撤销时，家庭网关从设备列表中删除该终端的标识和公钥，并将版本号更新，比如进行一次累加，再将更新后的版本号发送给该信任群组中其它未撤销的所有终端设备。这样，使得未被撤销的终端设备所保存的版本号是一致的，而被撤销后的终端设备的版本号与未被撤销的终端设备的版本号不同，比如小于未被撤销的终端设备的版本号。从而，在后续的终端设备之间的认证过程中，终端设备只需通过发送版本号则可进行简单的认证，从而提高了认证效率。

另外，为了使得认证更加严谨，家庭网关在每次更新后设备列表后，还可以将更新后的设备列表发送给所有未撤销的终端设备，终端设备对该设备列表进行存储。这样，使得终端设备相互认证时，及时对方所发送的版本号与自己所存储的版本号不相同，还可以通过判断所存储的设备列表中是否包含对方的记录信息，比如终端的标识，从而确定对方的身份是否有效。避免了有的终端设备比如由于离线的原因未能及时更新版本号，而导致被认为身份失效的情况，实现了离线认证。而且，终端设备在存储有设备列表的情况下，在判断了对方的版本号是否正确后，若设备列表中包含对方的标识和公钥，则终端设备还可以无需对方发送公钥，就可以进行预计算，从而提高了认证的效率。

需要说明的是，上述所描述的实例中是通过以家庭网关为服务器进行举例说明，在本

申请实施例中，服务器还可以为路由器、交换机、云端服务器等具备智能处理能力的服务性设备，本申请不做具体限制。主人终端可以为智能手机、笔记本电脑、个人电脑、智能手表等具有智能处理能力的终端设备。智能终端可以为智能灯泡、智能冰箱、智能空调等具有智能控制能力的设备，具体不做限定。

下面通过具体的实施例对本申请所提供的身份认证的方法进行详细描述，参照图 2 所示，图 2 实施例所描述的内容为当有终端加入信任群组时，服务器和终端对设备列表维护和版本号的更新的具体实现方式。

参照图 2 所示，本申请实施例中身份认证的方法的一个实施例包括：

101、当第一终端加入信任群组时，所述第一终端将所述第一终端的标识以及公钥发送给服务器。

102、服务器接收第一终端发送的标识和公钥。

当第一终端需要加入信任群组时，第一终端生成公私钥对，比如通过与服务器所约定的生成算法椭圆曲线数字签名算法（英文全称：Elliptic Curve Digital Signature Algorithm，英文缩写：ECDSA）生成公私钥对（Pkx，Skx）。第一终端在生成了公私钥对后，则向服务器发送入群请求，该请求则包含第一终端的公钥和第一终端的标识，即，第一终端将所生成的公钥 Pk 以及第一终端的标识，比如第一终端的 IDx 发送给服务器。可选的，为了提高在发送公钥和标识时的安全性，第一终端可以通过安全通道发送该入群请求。

103、服务器将接收到的所述第一终端的标识以及公钥存储在所述信任群组的设备列表中。

服务器中维护有一个设备列表，其中包含该信任群组中所有终端设备的公钥和标识，以及每个公钥和标识的对应关系。当有新的终端需要加入到该信任群组中时，服务器则将该终端的公钥、标识以及对应关系加入到该设备列表中，表示已经将该新的终端加入至信任群组中。

可选的，若服务器中维护了多个信任群组，比如可以划分为客厅群组、卧室群组、厨房群组等。服务器可以根据第一终端所发送的入群请求中所指示的群组名称将该第一终端的标识以及公钥加入至所选择的信任群组的设备列表中，或者服务器智能为该第一终端分配一个信任群组，并将该第一终端的标识和公钥加入所分配的信任群组中的设备列表中。

104、所述服务器根据当前的第一版本号为所述第一终端生成第一证书。

在本申请中，服务器还维护有一个版本号，该版本号可以是一个计数器，比如通过 counter 表示。当前的版本号，即表示当前服务器中所维护的 counter 的数值。由于版本号是会更新的，每个信任群组中的终端设备都应当接收服务器所发送的当前服务器所维护的最新的版本号，使得终端设备在进行互相认证时，可以通过根据对比对方版本号与自己所存储的版本号的大小来判断对方的身份是否有效。但是由于版本号只是一个简单的数值，很容易被恶意修改，如果只是通过版本号进行认证，可能导致错误的认证成功，因此服务器需要将当前的版本号为终端生成证书，使得终端在认证时，再次检查对方的证书中的版本号是否正确，或者通过版本号来判断对方的证书是否有效。

具体的，服务器先生成公私钥对 (Pkgw, Skgw)，通过私钥 Skgw 生成签名证书 T，以该签名 T 作为该第一终端的第一证书。可选的，服务器在生成签名证书时，还可以包含该第一终端所在的信任群组的名称标识 G-ID，该第一终端的公钥 Pkx 和该第一终端的标识 IDx，那么该签名证书 T 可以表示为 $T = \text{sign}(G-ID || (IDx, Pkx) || \text{counter})$ 。

105、所述服务器将所述第一证书以及所述第一版本号发送给所述第一终端。

106、第一终端接收服务器发送的第一证书以及第一版本号。

第一终端在接收到服务器发送的第一证书以及第一版本号后，则表示知道已经成功加入至信任群组中，第一终端则可以通过接收到的第一证书以及第一版本号与信任群组中的其它终端设备进行身份认证，从而进行指令控制等操作。比如第一终端为访客终端，该访客终端在成功加入至该信任群组中，则可以向智能灯泡发送认证请求，当智能灯泡根据版本号 and 证书确认该访客终端的身份有效后，该访客终端则可以向智能灯泡发起控制指令，比如开灯、关灯、调节亮度等控制指令。可选的，若服务器维护多个信任群组，且由服务器为该第一终端分配了群组，则该服务器还可以将所分配的群组的名称标识 G-ID 也发送给第一终端，以便后续终端设备之间认证时判断对方是否与自己处于同一信任群组中。

参照图 3 所示，图 3 实施例所描述的内容为当有终端从信任群组中撤销时，服务器以及终端对设备列表的维护以及版本号的更新的具体实现方式。

201、当第二终端从所述信任群组中撤销时，所述服务器删除所述设备列表中所述第二终端的标识以及公钥。

撤销终端的条件可以包括多种，比如主人终端向服务器发送指令，需要对信任群组中的第二终端进行撤销，或者，当服务器检测到第二终端存在病毒来源时，则可以主动执行撤销。当需要撤销该第二终端时，首先则需要删除设备列表中该第二终端的公钥和标识。

202、所述服务器按照预设规则更新所述第一版本号为第二版本号。

为了使得被撤销后的终端无法与该信任群组中其它终端不能成功认证身份，服务器需要更新第一版本号为第二版本号，比如将 counter 值进行累加一次，得到新的 counter 值。将新的版本号发送给未被撤销的其它终端后，及时当该被撤销后的第二终端与其它终端进行认证时，首先版本号则不会相同，从而不会认证成功。

203、所述服务器根据更新后的所述第二版本号为所述信任群组中未撤销的其它终端分别生成对应的第二证书。

为了防止本版本号被恶意修改，导致错误的认证成功的情况，服务器还需要根据更新后的版本号为每个未被撤销的终端分别生成新的证书，即上述的第二证书。这样，即使被撤销后的终端恶意修改版本号后，其并不能接收到服务器所生成的最新证书，因此，在进行证书对比时，不会认证成功。

204、所述服务器将所生成第二证书以及所述第二版本号分别发送给所对应的未撤销的终端，以使得未撤销的终端更新证书以及版本号。

205、设备列表中的终端接收所述服务器发送的第二证书以及第二版本号。

设备列表中的终端在接收到服务器发送的第二证书以及第二版本号后，则对之前所存储的证书以及版本号进行更新，保存最新的证书以及版本号，以便后续进行终端设备之间

认证时进行认证判断。可选的，为了提高在发送公钥和标识时的安全性，服务器也可以通过安全通道发送第二证书以及第二版本号。

在实际应用中，可能存在网络覆盖不全的地方，比如大门门锁、阳台灯泡等位置处可能网络信号较弱，从而导致服务器发送第二证书以及第二版本号至大门门锁和阳台灯泡失败，使得大门门锁和阳台灯泡无法及时更新至最新的证书以及版本号。在本申请实施例中，当服务器检测到发送第二证书和第二版本号失败时，则可以向特定的终端设备，比如主人终端发送指示信息，指示该主人终端进行接力更新，该指示信息中包含大门门锁、阳台灯泡的第二证书和第二版本号，主人终端在接收到该指示信息后，则提示用户使用主人终端进行接力更新，比如提示用户携带该主人终端移动至大门门锁和阳台灯泡的区域，通过主人终端将服务器所生成的大门门锁的第二证书和第二版本号发送给大门门锁设备，将服务器所生成的阳台灯泡的第二证书和第二版本号发送给阳台灯泡。这样，使得每次更新时，所有信任群组中的终端设备都能够更新至最新的版本号和证书。提高了认证的可靠性。

图 2 实施例描述了有新的终端加入信任群组时服务器对设备列表进行更新维护的一个实施例过程，在一种可能的实现方式中，每个终端设备也可以单独存储设备列表，服务器更新设备列表的信息后，还可以将更新后的设备列表发送给每个终端设备，以方便终端设备在认证过程中通过设备列表中获取对方的公钥从而进行预计算，提高认证效率。参照图 4 所示，图 4 实施例为当有新的终端加入信任群组时，服务器还将更新后的设备列表发送给列表中的所有终端的具体实现方式。

步骤 301~303 参照图 2 实施例中步骤 101~103，此处不做赘述。

304、所述服务器根据当前的第一版本号为所述第一终端生成第一证书。

在图 2 实施例中，服务器可以根据第一终端的标识和公钥、第一版本号、群组名称标识为第一终端生成签名证书，在本实施例中，由于信任群组中每个终端标识需要单独进行设备列表的存储，因此，为了提高证书的可靠性，服务器还可以根据群组名称标识、第一版本号以及设备列表的信息为该第一终端生成第一证书，其具体表达方式可以为 $T = \text{sign}(G-ID || (\{ID, Pk\}) || \text{counter})$ 。

305、所述服务器将所述第一证书、所述第一版本号以及所述设备列表发送给所述第一终端，其中，所述设备列表包含所述信任群组中所有未撤销的终端的标识以及公钥，以使得所述第一终端在认证过程中从所述设备列表中获取待认证终端的标识和公钥从而进行认证预计算。

在本申请实施例中，服务器不仅将第一证书以及第一版本号发送给第一终端，还将最新的设备列表也发送给第一终端，这样，使得第一终端在认证过程中，确认对方的版本号与自己所存储的版本号一致时，可以通过自己所存储的设备列表中对方的公钥信息进行预计算，比如在后续的通信认证过程中，无需对方发送公钥，则可以根据自己所存储的对方的公钥进行加密计算，从而提高了认证的效率。

306、所述服务器将存储有新增的第一终端的标识以及公钥的设备列表发送给所述信任群组中所有未撤销的其它终端。

由于信任群组中新增了新的终端的标识和公钥，服务器在更新了设备列表后，还可以将更新后的设备列表发送给该信任群组中所有未撤销的其它终端，以便其它终端所存储的设备列表中的信息为最新的信息。

需要说明的是，对于图 4 实施例的新的终端加入信任群组的实现方式所对应的从信任群组中撤销终端时的实现方式，与图 3 实施例的撤销过程相似，其区别的地方为包括，服务器生成第二证书时，可以为 $T = \text{sign}(G-ID || (\{ID, Pk\}) || \text{counter})$ ，其中， $\{ID, Pk\}$ 为删除了撤销的终端的标识和公钥的设备列表。另外，对于信任群组中未撤销的终端，服务器不仅将新生成的第二证书以及第二版本号发送给这些终端，服务器还需要将更新后的设备列表发送给这些终端。

上述实施例描述了新的终端如何加入信任群组中，以及如何从信任群组中撤销终端的过程的实现方式，下面对终端设备之间进行认证时的具体方式进行描述。

参照图 5 所示，本申请实施例中身份认证的方法的另一实施例包括：

401、第一终端接收第二终端发送的认证请求，所述认证请求包含第一版本号 and 所述第二终端的标识，所述第一版本号为服务器发送给所述第一终端的版本号，当有终端从信任群组中撤销时，服务器会对版本号进行累加，并将累加后的版本号发送给所述信任群组中所有未撤销的终端。

可选的，该认证请求中还可以包括第二终端的证书，即服务器发送给第二终端的证书，这样，第二终端的第一版本号与服务器一起发送给第一终端，提高了第二终端的版本号的可靠性。

402、所述第一终端判断所述第一版本号是否小于第二版本号，其中，所述第二版本号为所述第一终端所存储的服务器所发送的版本号。

由于服务器在每次更新版本号时是通过累加的方式进行更新的，若第一版本号小于第二版本号，则表示第一终端所存储的版本号是新的版本号，而第二终端所存储的版本号是旧的版本号，若第一版本号大于第二版本号，那么表示第二终端所存储的版本号是新的版本号，而第一终端所存储的版本号是旧的版本号。

403、当所述第一版本号小于所述第二版本号时，所述第一终端确定所述第二终端的身份失效。

当第一版本号小于第二版本号时，则表示第二终端未能更新到新的版本号，而服务器只有在没撤销一次终端时会更新一次版本号，因此该第二终端可能是被撤销过后的终端，所以第一终端可以确定第二终端的身份失效，无需进行后续的证书认证过程。这样，通过将对方的版本号与自己所存储的版本号进行对比，即能够判断出对方的身份是否有效，无需如现有技术一样从撤销列表中确定对方的身份，减少了通信的流程以及信息量，提高了认证的效率。

可选的，当第一版本号大于或等于第二版本号时，第一终端则可以进行后续的通信认证，包括：要求第二终端发送第二终端的公钥和证书，第一终端先通过服务器的公钥验证该证书是否是服务器发送给第二终端的，若否，则认证失败；若是，则第一终端再通过该公钥与第一终端的私钥进行加密计算，将加密后的数据包发送给第二终端进行通信认证，

若第二终端能够解析出该加密的数据包，则认证成功。

这样，通过本申请所提供的认证方式，减少了通信交互，提高了认证的效率。同时在认证过程中，无需服务器的参与，实现了离线认证。

另一种实现方式中，每个终端设备存储有服务器所发送的设备列表，该设备列表中包含所有未撤销的终端的标识和公钥。参照图 6 所示，本申请实施例中身份认证的方法的另一实施例包括：

501、第一终端接收第二终端发送的认证请求。

502、第一终端判断所述第一版本号是否小于或等于第二版本号，若是，则执行步骤 503；如否，则执行步骤 505。

503、当所述第一版本号小于或等于所述第二版本号时，所述第一终端判断所述设备列表中是否包含所述第二终端的记录信息。

由于在实际应用中，有的终端设备由于区域或者其它原因，不处于网络覆盖区，从而可能导致服务器更新了证书和版本号，但是这写设备由于网络原因而不能及时更新。对于这种情况，因为第一终端存储有服务器发送的设备列表，设备列表中包含所述信任群组中所有未撤销的终端的标识和公钥，第一终端则可以根据第二终端的标识查找自己所存储的设备列表中是否同样包含该第二终端的标识的记录，从而确定第二终端是否已经被撤销。

504、当所述设备列表中不包含所述第二终端的记录信息时，所述第一终端确定所述第二终端的身份失效。

若设备列表中不包含第二终端的记录信息，即没有第二终端的标识和公钥，则表示该第二终端是被撤销了的或者从而加入该信任群组的终端设备，从而认定该第二终端的身份失效。

可选的，当所述第一终端确定所述设备列表中包含所述第二终端的记录信息时，本申请实施例还可以包括：所述第一终端从所述设备列表中获取所述第二终端的公钥，并通过所述第二终端的公钥与所述第二终端进行通信认证。

当设备列表中包含第二终端的记录信息，则表示第二终端的身份认证通过，则可以执行后续的通信认证，此时，无需第二终端发送第二终端的公钥给第一终端，第一终端可以直接从设备列表中获取第二终端的公钥进行通信认证。通信认证是指第一终端在确认第二终端未被服务器从信任群组中撤销时，或者确定第二终端的证书是服务器生成的证书时，则通过第二终端的公钥进行加密数据包，从而发送给第二终端，由第二终端进行解析数据包并认证的过程。

505、当所述第一版本号大于所述第二版本号时，所述第一终端接收所述第二终端发送的第二证书以及公钥。

当第二终端的版本号大于第一终端的版本号时，第一终端需要获取第二终端的公钥，并且在后续的通信认证过程中，使用该公钥进行通信加密认证。

在这种情况下，可能是第一终端并未更新设备列表，而第二终端为最新加入该信任群组的终端设备，因此，第一终端无需从设备列表中查找是否有该第二终端的记录信息。因此需要要求第二终端发送第二终端的公钥给第一终端。

506、所述第一终端根据所述服务器的公钥验证所述第二证书是否为所述服务器发送给第二终端的证书。

服务器的公钥可以为第一终端预先获取到的，比如服务器在生成公私钥对后，将公钥广播给所有终端设备，也可以为服务器在发送证书和版本号给终端时，同时将服务器的公钥发送给终端的。

为了防止第二终端给第一终端发送的证书是假的证书，即不是服务器发送的证书，因此，第一终端需要对该证书进行验证，只有当该第二证书是服务器通过服务器的私钥所生成的签名证书，验证才会正确。

507、当所述第一终端确定所述第二证书不为所述服务器发送给第二终端的证书时，所述第一终端确定所述第二终端的身份失效。

当所述第一终端验证所述第二证书不为所述服务器发送给第二终端的证书时，则表示该第二终端发送给第一终端的证书不是服务器所发送给第二终端的证书，因此，第一终端可以确定第二终端的身份不安全，或者失效，无需进行后续的通信认证过程。

可选的，当第一终端验证第二终端的第二证书正确时，则第一终端在后续的通信认证过程中，第一终端使接收第二终端发送的所述第二终端的公钥，并通过所述第二终端的公钥与所述第二终端进行通信认证。

参照图 7 所示，本申请实施例中服务器的一个实施例包括：

生成单元 601，用于当接收第一终端发送的加入信任群组的入群请求时，根据第一版本号为所述第一终端生成第一证书；

发送单元 602，用于向第一终端发送所述第一证书以及所述第一版本号；

更新单元 603，用于当确认第二终端从所述信任群组中撤销时，所述服务器按照预设规则更新所述第一版本号为第二版本号；

所述生成单元 601 还用于，根据所述第二版本号为所述信任群组中未撤销的终端分别生成对应的第二证书；

所述发送单元 602 还用于，向所述信任群组中未撤销的终端分别发送对应的第二证书以及所述第二版本号。

可选的，所述入群请求包含所述第一终端的标识和公钥；所述服务器还包括：

存储单元 604，用于将所述第一终端的标识和公钥存储于设备列表中；

所述发送单元 602 还用于，将所述设备列表发送给第一终端；其中，所述设备列表包含所述信任群组中所有未撤销的终端的标识以及公钥，以使得所述第一终端在认证过程中从所述设备列表中获取待认证终端的公钥从而进行认证处理。

可选的，所述发送单元 602 还用于：

向所述信任群组中所有未撤销的终端发送存储有新增的第一终端的标识以及公钥的设备列表。

图 7 实施例的具体描述参照图 2 至图 4 实施例中身份认证的方法的描述内容，此处不做赘述。

参照图 8 所示，图 8 实施例为本申请实施例中终端为第一终端时的一个实施例，包

括:

发送单元 701, 用于向服务器发送加入信任群组的入群请求, 所述入群请求包含所述第一终端的标识和公钥;

接收单元 702, 用于接收所述服务器发送的第一证书以及第一版本号, 其中所述第一证书为所述服务器根据所述第一版本号为所述第一终端所生成的证书;

所述接收单元 702 还用于, 当第二终端从所述信任群组中撤销时, 接收所述服务器发送的第二证书以及第二版本号, 其中, 第二版本号为所述服务器按照预设规则所更新的版本号, 所述第二证书为所述服务器根据所述第二版本号为所述第一终端所生成的证书。

可选的, 所述接收单元 702 还用于:

接收所述服务器发送的设备列表, 其中, 所述设备列表包含所述信任群组中所有未撤销的终端的标识以及公钥, 以使得所述第一终端在认证过程中从所述设备列表中获取待认证终端的公钥从而进行认证处理。

图 8 实施例的具体描述参照图 2 至图 4 实施例中身份认证的方法的描述内容, 此处不做赘述。

参照图 9 所示, 本申请实施例中终端的另一实施例包括:

接收单元 801, 用于接收第二终端发送的认证请求, 所述认证请求包含第一版本号和所述第二终端的标识, 所述第一版本号为服务器发送给所述第一终端的版本号, 当有终端从信任群组中撤销时, 服务器会对版本号进行累加, 并将累加后的版本号发送给所述信任群组中所有未撤销的终端;

判断单元 802, 用于判断所述第一版本号是否小于第二版本号, 其中, 所述第二版本号为所述第一终端所存储的服务器所发送的版本号;

确定单元 803, 用于当确定所述第一版本号小于所述第二版本号时, 所述第一终端确定所述第二终端的身份失效。

可选的, 所述第一终端存储有所述服务器发送的设备列表, 所述设备列表中包含所述信任群组中所有未撤销的终端的标识和公钥;

所述判断单元 802 还用于, 当确定所述第一版本号小于或等于所述第二版本号时, 判断所述设备列表中是否包含所述第二终端的记录信息;

所述确定单元 803 还用于, 当确定所述设备列表中不包含所述第二终端的记录信息时, 确定所述第二终端的身份失效。

可选的, 所述第一终端存储有所述服务器发送的设备列表, 所述设备列表中包含所述信任群组中所有未撤销的终端的标识和公钥;

所述接收单元 801 还用于, 当所述第一终端确定所述第一版本号大于所述第二版本号时, 接收所述第二终端发送的第二证书;

所述终端还包括:

验证单元 804, 用于根据所述服务器的公钥验证所述第二证书是否为所述服务器发送给第二终端的证书;

所述确定单元 803 还用于, 当确定所述第二证书不为所述服务器发送给第二终端的证

书时，确定所述第二终端的身份失效。

图 9 实施例的具体描述参照图 5 至图 6 实施例中身份认证的方法的描述内容，此处不做赘述。

图 7 实施例所述的服务器还有另一个形式的实施例，参照图 10 所示，包括：处理器 901、存储器 902、收发器 903，所述处理器 901、所述存储器 902 以及所述收发器 903 通过总线 904 连接，收发器 903 可以包括发送器与接收器，所述存储器 902 存储有计算机指令，所述处理器 901 通过执行所述计算机指令用于实现图 2 至图 4 实施例中身份认证的方法中服务器所执行的功能。具体的实现可以采用各类灵活的设计方式，各个器件相应的功能可以进一步的参考方法实施例，本申请不做限制。

图 8 以及图 9 实施例所述的服务器还有另一个形式的实施例，参照图 11 所示，包括：处理器 1001、存储器 1002、收发器 1003，所述处理器 1001、所述存储器 1002 以及所述收发器 1003 通过总线 1004 连接，收发器 1003 可以包括发送器与接收器，所述存储器 1002 存储有计算机指令，所述处理器 1001 通过执行所述计算机指令用于实现图 2 至图 6 实施例中身份认证的方法中终端所执行的功能。具体的实现可以采用各类灵活的设计方式，各个器件相应的功能可以进一步的参考方法实施例，本申请不做限制。

参照图 12 所示，本申请实施例还提供了一种身份认证的系统 100，包括：服务器 1101、第一终端 1102 以及第二终端 1103；

所述第一终端 1102 用于，向所述服务器 1101 发送请求加入信任群组的入群请求；

所述服务器 1101 用于，根据第一版本号为所述第一终端 1102 生成第一证书；

所述服务器 1101 还用于，向第一终端 1102 发送所述第一证书以及所述第一版本号；

所述第一终端 1102 还用于，接收所述服务器 1101 发送的第一证书以及第一版本号；

当所述服务器 1101 确认所述第二终端 1103 从所述信任群组中撤销时，所述服务器 1101 还用于，按照预设规则更新所述第一版本号为第二版本号；

所述服务器 1101 还用于，根据所述第二版本号为所述信任群组中未撤销的终端分别生成对应的第二证书；

所述服务器 1101 还用于，向所述信任群组中未撤销的终端分别发送对应的第二证书以及所述第二版本号；

所述第一终端 1102 还用于，接收所述服务器 1101 发送的第二证书以及第二版本号。

可选的，所述入群请求包含所述第一终端的标识和公钥；

所述服务器 1101 还用于，将所述第一终端 1102 的标识和公钥存储于设备列表中，并将所述设备列表发送给第一终端 1102；其中，所述设备列表包含所述信任群组中所有未撤销的终端的标识以及公钥，以使得所述第一终端 1102 在认证过程中从所述设备列表中获取待认证终端的公钥从而进行认证处理；

所述第一终端还用于，接收所述服务器 1101 发送的设备列表。

可选的，所述服务器 1101 还用于，向所述信任群组中所有未撤销的终端发送存储有新增的第一终端 1102 的标识以及公钥的设备列表。

在上述实施例中，可以全部或部分地通过软件、硬件、固件或者其任意组合来实现。

当使用软件实现时，可以全部或部分地以计算机程序产品的形式实现。

所述计算机程序产品包括一个或多个计算机指令。在计算机上加载和执行所述计算机程序指令时，全部或部分地产生按照本发明实施例所述的流程或功能。所述计算机可以是通用计算机、专用计算机、计算机网络、或者其他可编程装置。所述计算机指令可以存储在计算机可读存储介质中，或者从一个计算机可读存储介质向另一计算机可读存储介质传输，例如，所述计算机指令可以从一个网站站点、计算机、服务器或数据中心通过有线（例如同轴电缆、光纤、数字用户线（DSL））或无线（例如红外、无线、微波等）方式向另一个网站站点、计算机、服务器或数据中心进行传输。所述计算机可读存储介质可以是计算机能够存储的任何可用介质或者是包含一个或多个可用介质集成的服务器、数据中心等数据存储设备。所述可用介质可以是磁性介质，（例如，软盘、硬盘、磁带）、光介质（例如，DVD）、或者半导体介质（例如固态硬盘 Solid State Disk(SSD)）等。

在本申请所提供的几个实施例中，应该理解到，所揭露的系统，装置和方法，可以通过其它的方式实现。例如，以上所描述的装置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，例如多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另一点，所显示或讨论的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，装置或单元的间接耦合或通信连接，可以是电性，机械或其它的形式。

所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者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者全部单元来实现本实施例方案的目的。

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。

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，可以存储在一个计算机可读存储介质中。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）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（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。

-17-

权 利 要 求

1、一种身份认证的方法，其特征在于，所述方法包括：

当服务器接收第一终端发送的加入信任群组的入群请求时，所述服务器根据第一版本号所述第一终端生成第一证书；

5 所述服务器向第一终端发送所述第一证书以及所述第一版本号；

当所述服务器确认第二终端从所述信任群组中撤销时，所述服务器按照预设规则更新所述第一版本号为第二版本号；

所述服务器根据所述第二版本号为所述信任群组中未撤销的终端分别生成对应的第二证书；

10 所述服务器向所述信任群组中未撤销的终端分别发送对应的第二证书以及所述第二版本号。

2、根据权利要求 1 所述的方法，其特征在于，所述入群请求包含所述第一终端的标识和公钥；所述方法还包括：

15 所述服务器将所述第一终端的标识和公钥存储于设备列表中，并将所述设备列表发送给第一终端；其中，所述设备列表包含所述信任群组中所有未撤销的终端的标识以及公钥，以使得所述第一终端在认证过程中从所述设备列表中获取待认证终端的公钥从而进行认证处理。

3、根据权利要求 2 所述的方法，其特征在于，所述方法还包括：

20 所述服务器向所述信任群组中所有未撤销的终端发送存储有新增的第一终端的标识以及公钥的设备列表。

4、一种身份认证的方法，其特征在于，所述方法包括：

第一终端向服务器发送请求加入信任群组的入群请求；

所述第一终端接收所述服务器发送的第一证书以及第一版本号，其中所述第一证书为所述服务器根据所述第一版本号为所述第一终端所生成的证书；

25 当第二终端从所述信任群组中撤销时，所述第一终端接收所述服务器发送的第二证书以及第二版本号，其中，第二版本号为所述服务器按照预设规则所更新的版本号，所述第二证书为所述服务器根据所述第二版本号为所述第一终端所生成的证书。

5、根据权利要求 4 所述的方法，其特征在于，所述方法还包括：

30 所述第一终端接收所述服务器发送的设备列表，其中，所述设备列表包含所述信任群组中所有未撤销的终端的标识以及公钥，以使得所述第一终端在认证过程中从所述设备列表中获取待认证终端的公钥从而进行认证处理。

6、一种身份认证的方法，其特征在于，所述方法包括：

35 第一终端接收第二终端发送的认证请求，所述认证请求包含第一版本号，当有终端从信任群组中撤销时，所述服务器会对版本号进行累加，并将累加后的版本号发送给所述信任群组中所有未撤销的终端；

所述第一终端判断所述第一版本号是否小于第二版本号，其中，所述第二版本号为所述服务器发送给所述第一终端的最新版本号；

当所述第一终端确定所述第一版本号小于所述第二版本号时，所述第一终端确定所述第二终端的身份失效。

7、根据权利要求6所述的方法，其特征在于，所述第一终端存储有所述服务器发送的设备列表，所述设备列表中包含所述信任群组中所有未撤销的终端的记录信息；

5 当所述第一终端确定所述第一版本号小于或等于所述第二版本号时，所述方法还包括：

所述第一终端判断所述设备列表中是否包含所述第二终端的记录信息；

当确定所述设备列表中不包含所述第二终端的记录信息时，所述第一终端确定所述第二终端的身份失效。

10 8、根据权利要求7所述的方法，其特征在于，所述方法还包括：

当确定所述设备列表中包含所述第二终端的记录信息时，所述第一终端从所述设备列表中获取所述第二终端的公钥，并通过所述第二终端的公钥与所述第二终端进行通信认证。

9、根据权利要求6至8任一所述的方法，其特征在于，所述方法还包括：

15 当确定所述第一版本号大于所述第二版本号时，所述第一终端接收所述第二终端发送的第二证书；

所述第一终端根据所述服务器的公钥验证所述第二证书是否为所述服务器发送给第二终端的证书；

20 当确定所述第二证书不为所述服务器发送给第二终端的证书时，所述第一终端确定所述第二终端的身份失效。

10、根据权利要求9所述的方法，其特征在于，所述方法还包括：

当确定所述第二证书为所述服务器发送给第二终端的证书时，所述第一终端接收所述第二终端发送的所述第二终端的公钥，并通过所述第二终端的公钥与所述第二终端进行通信认证。

25 11、一种服务器，其特征在于，所述服务器包括：

生成单元，用于当接收第一终端发送的加入信任群组的入群请求时，根据第一版本号为所述第一终端生成第一证书；

发送单元，用于向第一终端发送所述第一证书以及所述第一版本号；

30 更新单元，用于当确认第二终端从所述信任群组中撤销时，所述服务器按照预设规则更新所述第一版本号为第二版本号；

所述生成单元还用于，根据所述第二版本号为所述信任群组中未撤销的终端分别生成对应的第二证书；

所述发送单元还用于，向所述信任群组中未撤销的终端分别发送对应的第二证书以及所述第二版本号。

35 12、根据权利要求11所述的服务器，其特征在于，所述入群请求包含所述第一终端的标识和公钥；所述服务器还包括：

存储单元，用于将所述第一终端的标识和公钥存储于设备列表中；

所述发送单元还用于，将所述设备列表发送给第一终端；其中，所述设备列表包含所述信任群组中所有未撤销的终端的标识以及公钥，以使得所述第一终端在认证过程中从所述设备列表中获取待认证终端的公钥从而进行认证处理。

13、根据权利要求 12 所述的服务器，其特征在于，所述发送单元还用于：

向所述信任群组中所有未撤销的终端发送存储有新增的第一终端的标识以及公钥的设备列表。

14、一种终端，其特征在于，当所述终端为第一终端时，所述终端包括：

发送单元，用于向服务器发送请求加入信任群组的入群请求；

接收单元，用于接收所述服务器发送的第一证书以及第一版本号，其中所述第一证书为所述服务器根据所述第一版本号为所述第一终端所生成的证书；

所述接收单元还用于，当第二终端从所述信任群组中撤销时，接收所述服务器发送的第二证书以及第二版本号，其中，第二版本号为所述服务器按照预设规则所更新的版本号，所述第二证书为所述服务器根据所述第二版本号为所述第一终端所生成的证书。

15、根据权利要求 14 所述的终端，其特征在于，所述接收单元还用于：

接收所述服务器发送的设备列表，其中，所述设备列表包含所述信任群组中所有未撤销的终端的标识以及公钥，以使得所述第一终端在认证过程中从所述设备列表中获取待认证终端的公钥从而进行认证处理。

16、一种终端，其特征在于，当所述终端为第一终端时，所述终端包括：

接收单元，用于接收第二终端发送的认证请求，所述认证请求包含第一版本，当有终端从信任群组中撤销时，所述服务器会对版本号进行累加，并将累加后的版本号发送给所述信任群组中所有未撤销的终端；

判断单元，用于判断所述第一版本号是否小于第二版本号，其中，所述第二版本号为所述服务器所发送给所述第一终端的最新版本号；

确定单元，用于当确定所述第一版本号小于所述第二版本号时，所述第一终端确定所述第二终端的身份失效。

17、根据权利要求 16 所述的终端，其特征在于，所述第一终端存储有所述服务器发送的设备列表，所述设备列表中包含所述信任群组中所有未撤销的终端的记录信息；

所述判断单元还用于，当确定所述第一版本号小于或等于所述第二版本号时，判断所述设备列表中是否包含所述第二终端的记录信息；

所述确定单元还用于，当确定所述设备列表中不包含所述第二终端的记录信息时，确定所述第二终端的身份失效。

18、根据权利要求 17 所述的终端，其特征在于，所述终端还包括：

获取单元，用于当确定所述设备列表中包含所述第二终端的记录信息时，从所述设备列表中获取所述第二终端的公钥；

认证单元，用于通过所述第二终端的公钥与所述第二终端进行通信认证。

19、根据权利要求 16 至 18 任一所述的终端，其特征在于，

所述接收单元还用于，当所述第一终端确定所述第一版本号大于所述第二版本号时，

—20—

接收所述第二终端发送的第二证书；

所述终端还包括：

验证单元，用于根据所述服务器的公钥验证所述第二证书是否为所述服务器发送给第二终端的证书；

5 所述确定单元还用于，当确定所述第二证书不为所述服务器发送给第二终端的证书时，确定所述第二终端的身份失效。

20、根据权利要求 19 所述的终端，其特征在于，

所述接收单元还用于：当确定所述第二证书为所述服务器发送给第二终端的证书时，接收所述第二终端发送的所述第二终端的公钥；

10 所述终端还包括：

认证单元，用于通过所述第二终端的公钥与所述第二终端进行通信认证。

21、一种身份认证的系统，其特征在于，包括：如权利要求 11 至 13 任一所述的服务器，以及权利要求 14 或 15 所述的终端。

15

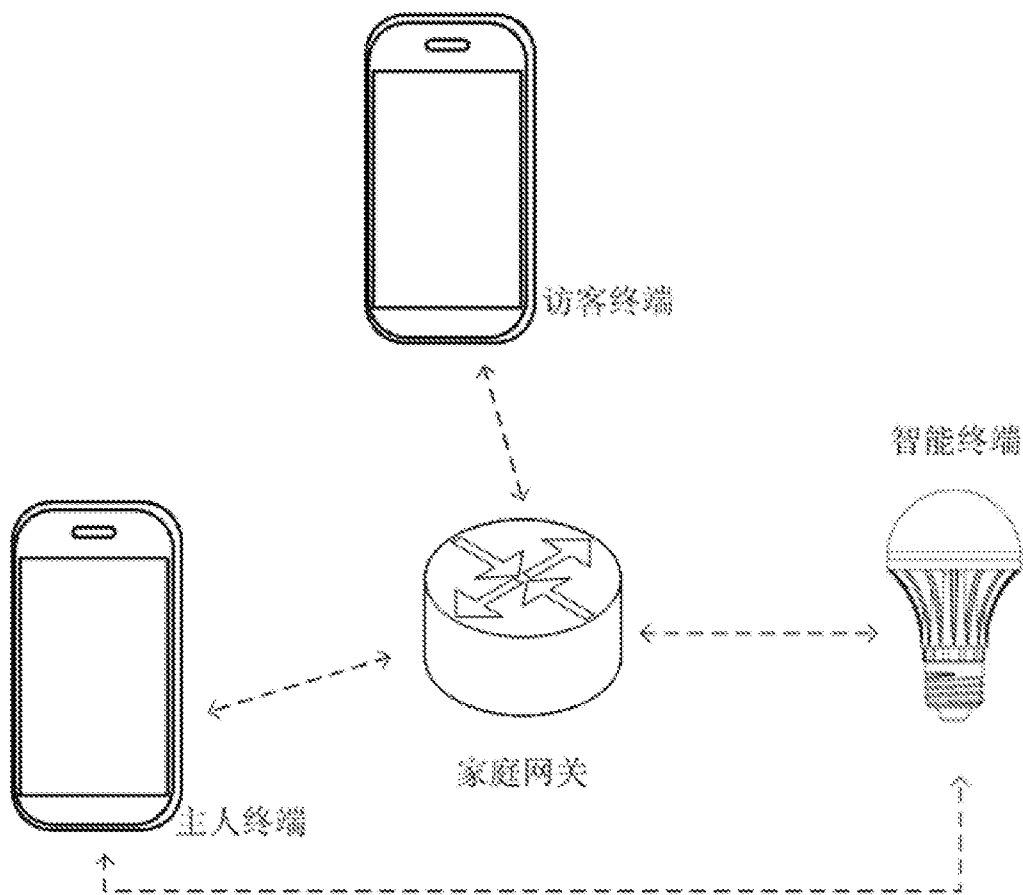


图 1

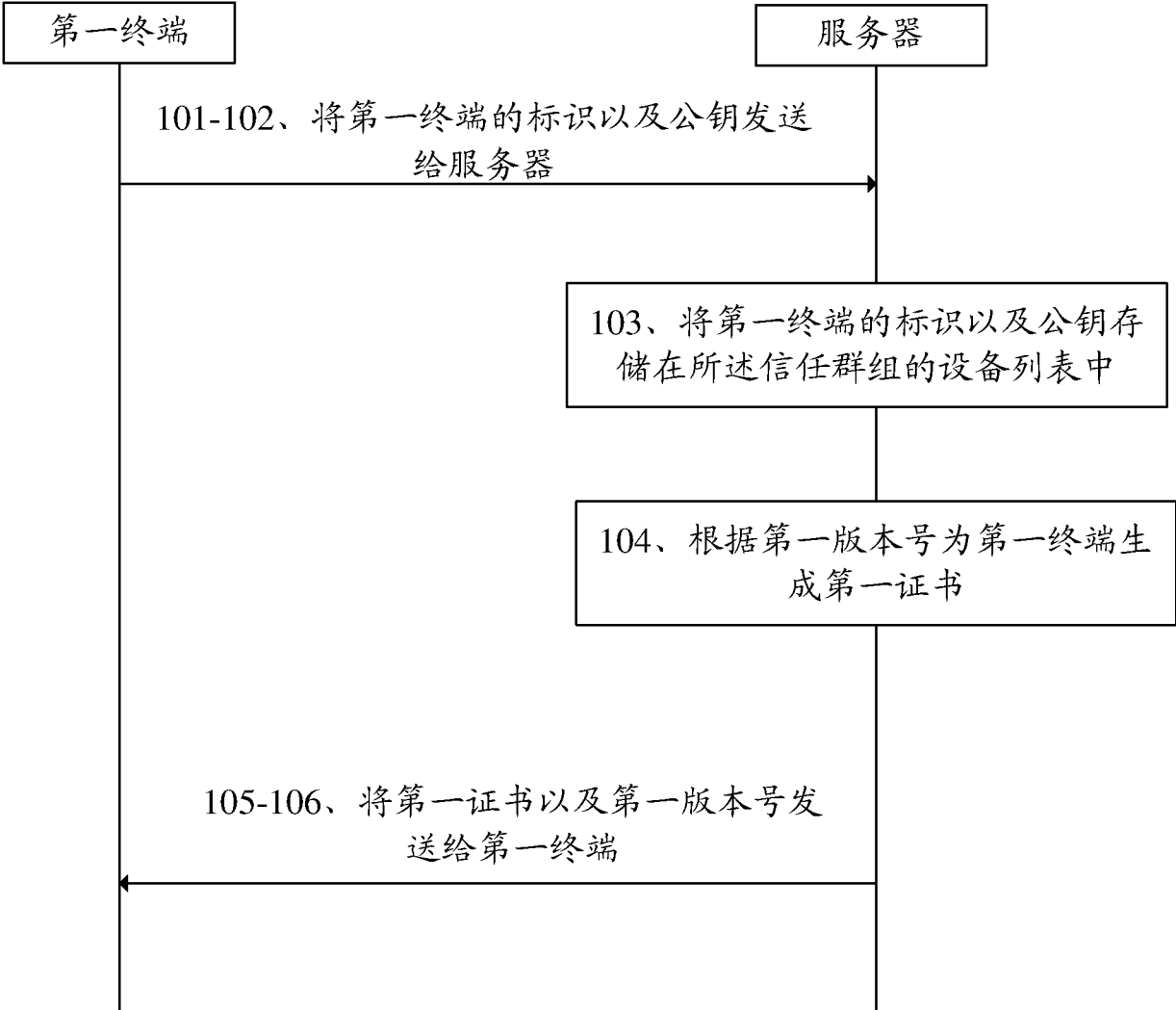


图 2

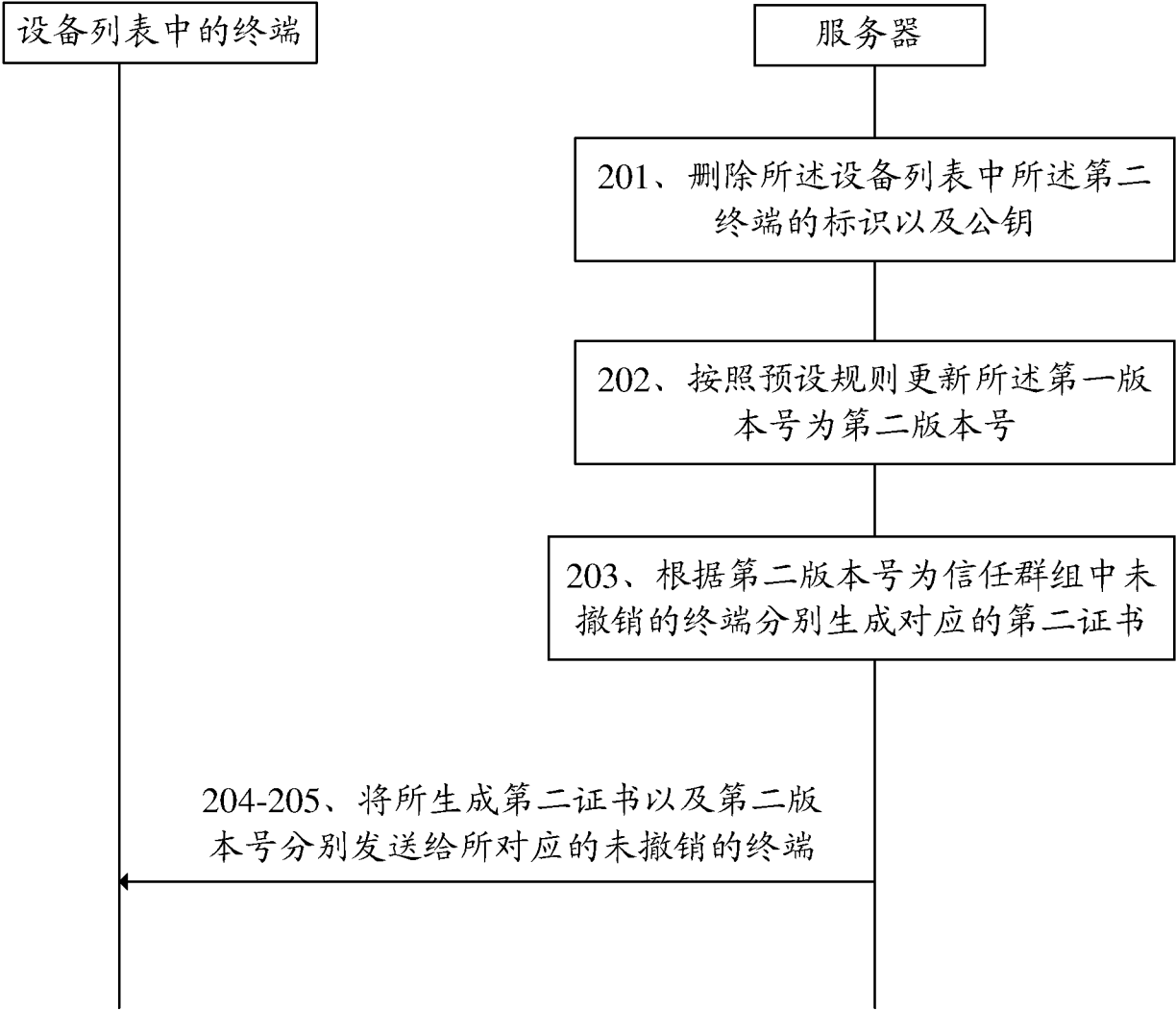


图 3

-4/7-

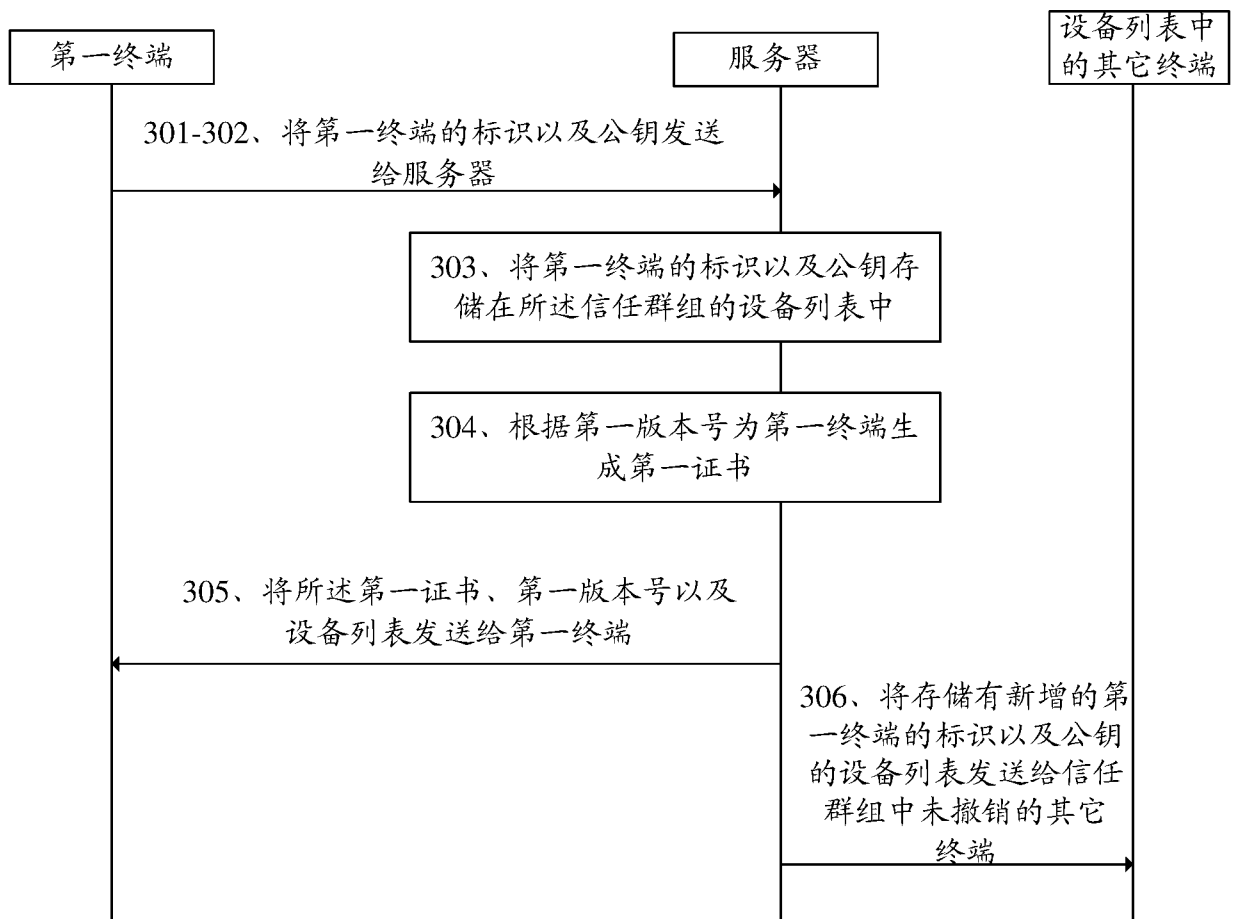


图 4

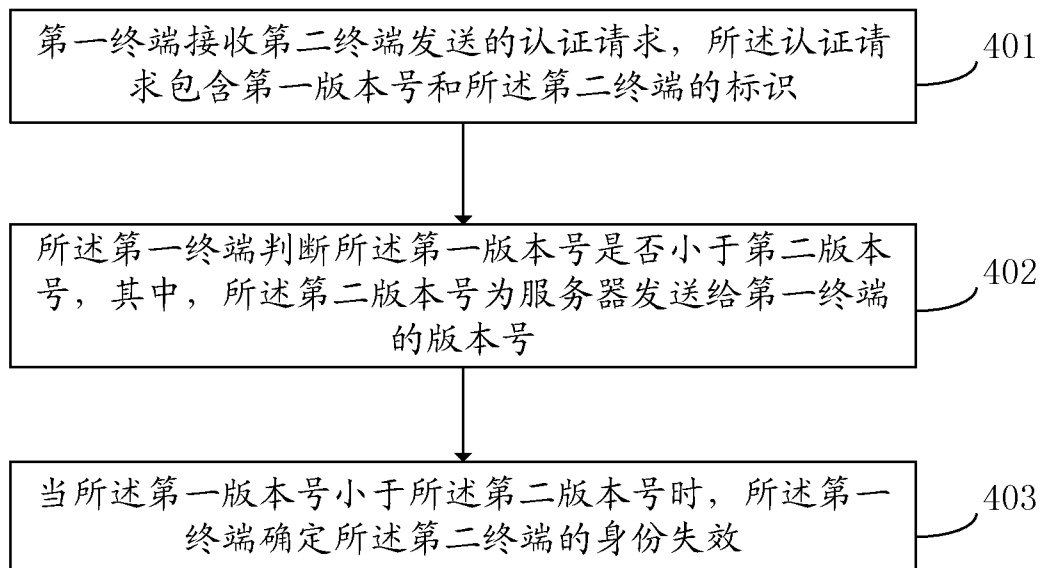


图 5

- 5/7 -

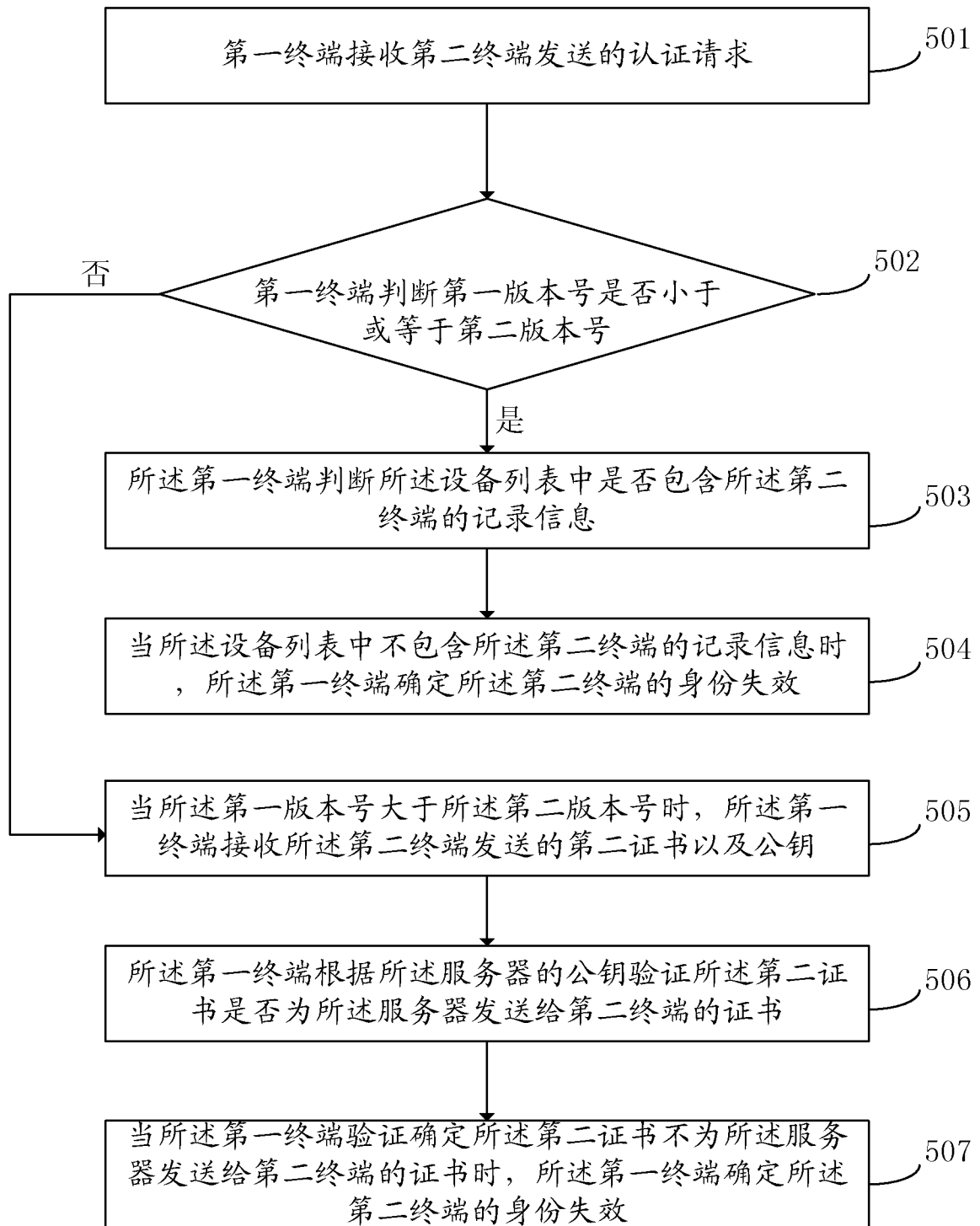


图 6

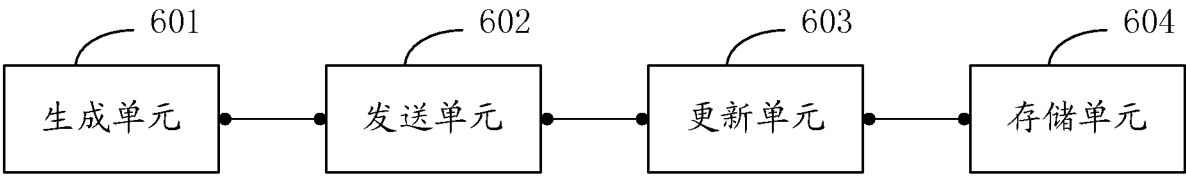


图 7

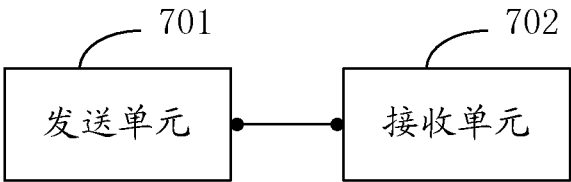


图 8

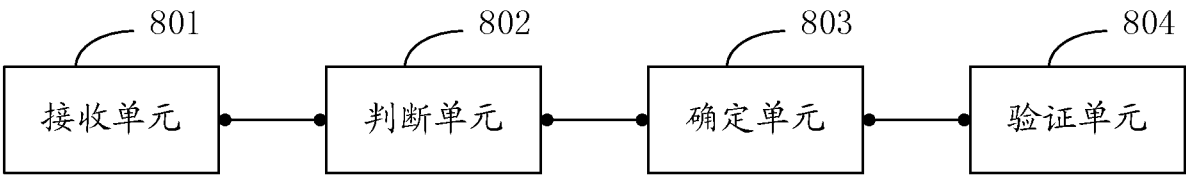


图 9

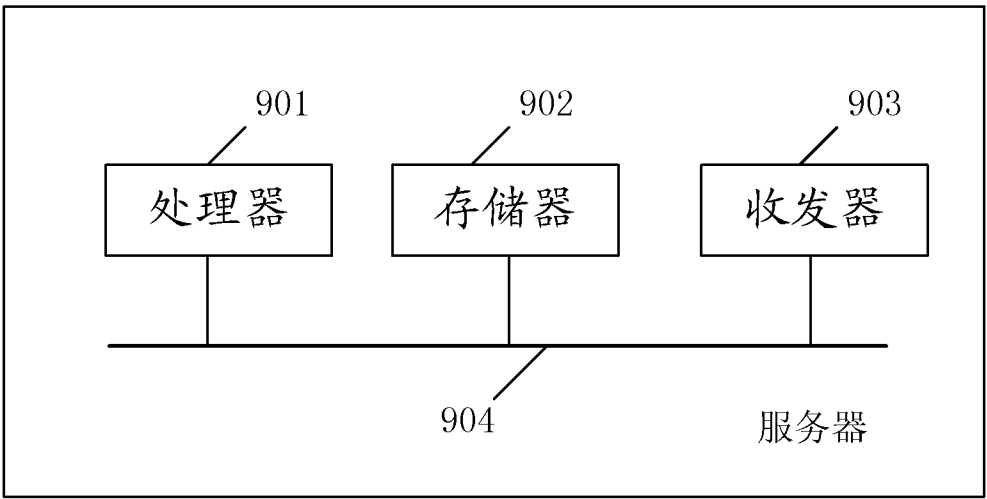


图 10

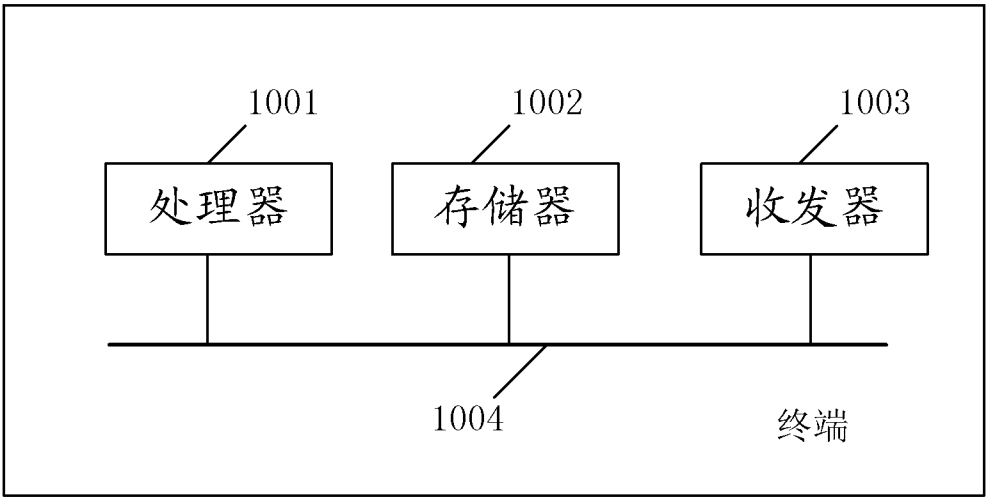


图 11

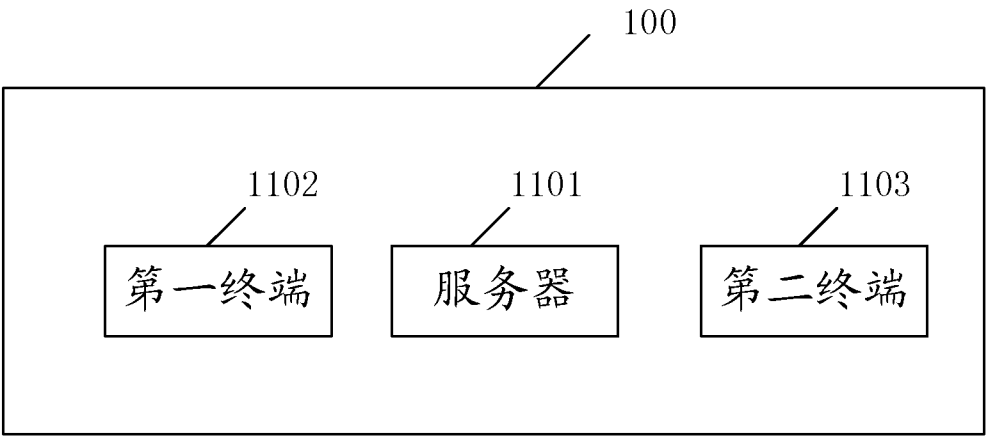


图 12

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2018/079283

A. CLASSIFICATION OF SUBJECT MATTER

H04L 12/28 (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 G06F

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)

WPI, EPODOC, CNPAT, CNKI: 身份, 认证, 鉴权, 证书, 版本, 刷新, 更新, 加入, 进入, 撤销, 退出, 离开, 群, 组, 请求, identity, authenticat+, certificate, version, update, join, enter, enlist, cancel, leave, depart, exit, quit, cluster, group, team, request

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 1859246 A (HUAWEI TECHNOLOGIES CO., LTD.), 08 November 2006 (08.11.2006), description, page 9, penultimate paragraph to page 11, paragraph 1	1-21
A	CN 103533403 A (INSTITUTE OF INFORMATION ENGINEERING, CHINESE ACADEMY OF SCIENCES), 22 January 2014 (22.01.2014), entire document	1-21
A	CN 102404347 A (NANJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS), 04 April 2012 (04.04.2012), entire document	1-21
A	CN 102420690 A (ASAT CHINA TECHNOLOGY INC.), 18 April 2012 (18.04.2012), entire document	1-21
A	US 2011225409 A1 (SIBERT, H. et al.), 15 September 2011 (15.09.2011), entire document	1-21

☐ 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	“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
“E” earlier application or patent but published on or after the international filing date	“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
“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)	“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
“O” document referring to an oral disclosure, use, exhibition or other means	“&” document member of the same patent family
“P” document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search 27 April 2018	Date of mailing of the international search report 24 May 2018
Name and mailing address of the ISA 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 WANG, Xin Telephone No. 86-(10)-53961617

International application No.
PCT/CN2018/079283

Form PCT/ISA/210 (patent family annex) (January 2015)

国际检索报告

国际申请号

PCT/CN2018/079283

A. 主题的分类 H04L 12/28 (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 G06F 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)) WPI, EPODOC, CNPAT, CNKI: 身份, 认证, 鉴权, 证书, 版本, 刷新, 更新, 加入, 进入, 撤销, 退出, 离开, 群, 组, 请求, identity, authenticat+, certificate, version, update, join, enter, enlist, cancel, leave, depart, exit, quit, cluster, group, team, request																				
C. 相关文件 <table border="1"> <thead> <tr> <th>类 型*</th> <th>引用文件, 必要时, 指明相关段落</th> <th>相关的权利要求</th> </tr> </thead> <tbody> <tr> <td>X</td> <td>CN 1859246 A (华为技术有限公司) 2006年 11月 8日 (2006 - 11 - 08) 说明书第9页倒数2段-第11页第1段</td> <td>1-21</td> </tr> <tr> <td>A</td> <td>CN 103533403 A (中国科学院信息工程研究所) 2014年 1月 22日 (2014 - 01 - 22) 全文</td> <td>1-21</td> </tr> <tr> <td>A</td> <td>CN 102404347 A (南京邮电大学) 2012年 4月 4日 (2012 - 04 - 04) 全文</td> <td>1-21</td> </tr> <tr> <td>A</td> <td>CN 102420690 A (上海可鲁系统软件有限公司) 2012年 4月 18日 (2012 - 04 - 18) 全文</td> <td>1-21</td> </tr> <tr> <td>A</td> <td>US 2011225409 A1 (SIBERT, HERVE等) 2011年 9月 15日 (2011 - 09 - 15) 全文</td> <td>1-21</td> </tr> </tbody> </table>			类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求	X	CN 1859246 A (华为技术有限公司) 2006年 11月 8日 (2006 - 11 - 08) 说明书第9页倒数2段-第11页第1段	1-21	A	CN 103533403 A (中国科学院信息工程研究所) 2014年 1月 22日 (2014 - 01 - 22) 全文	1-21	A	CN 102404347 A (南京邮电大学) 2012年 4月 4日 (2012 - 04 - 04) 全文	1-21	A	CN 102420690 A (上海可鲁系统软件有限公司) 2012年 4月 18日 (2012 - 04 - 18) 全文	1-21	A	US 2011225409 A1 (SIBERT, HERVE等) 2011年 9月 15日 (2011 - 09 - 15) 全文	1-21
类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求																		
X	CN 1859246 A (华为技术有限公司) 2006年 11月 8日 (2006 - 11 - 08) 说明书第9页倒数2段-第11页第1段	1-21																		
A	CN 103533403 A (中国科学院信息工程研究所) 2014年 1月 22日 (2014 - 01 - 22) 全文	1-21																		
A	CN 102404347 A (南京邮电大学) 2012年 4月 4日 (2012 - 04 - 04) 全文	1-21																		
A	CN 102420690 A (上海可鲁系统软件有限公司) 2012年 4月 18日 (2012 - 04 - 18) 全文	1-21																		
A	US 2011225409 A1 (SIBERT, HERVE等) 2011年 9月 15日 (2011 - 09 - 15) 全文	1-21																		
☐ 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 4月 27日		国际检索报告邮寄日期 2018年 5月 24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 王欣 电话号码 86-(10)-53961617																		

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2018/079283

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	1859246	A	2006年 11月 8日	无			
CN	103533403	A	2014年 1月 22日	无			
CN	102404347	A	2012年 4月 4日	无			
CN	102420690	A	2012年 4月 18日	无			
US	2011225409	A1	2011年 9月 15日	EP	2545484	A2	2013年 1月 16日
				WO	2011110449	A2	2011年 9月 15日