

(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
2021 年 9 月 23 日 (23.09.2021)



(10) 国际公布号
WO 2021/184865 A1

(51) 国际专利分类号:
H04L 9/00 (2006.01)

(21) 国际申请号: PCT/CN2020/137283

(22) 国际申请日: 2020 年 12 月 17 日 (17.12.2020)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202010193435.8 2020年3月18日 (18.03.2020) CN

(71) 申请人: 大唐移动通信设备有限公司 (DATANG MOBILE COMMUNICATIONS EQUIPMENT CO., LTD) [CN/CN]; 中国北京市海淀区学院路29号, Beijing 100083 (CN)。

(72) 发明人: 周巍 (ZHOU, Wei); 中国北京市海淀区学院路29号, Beijing 100083 (CN)。

(74) 代理人: 北京路浩知识产权代理有限公司 (CN-KNOWHOW INTELLECTUAL PROPERTY AGENT

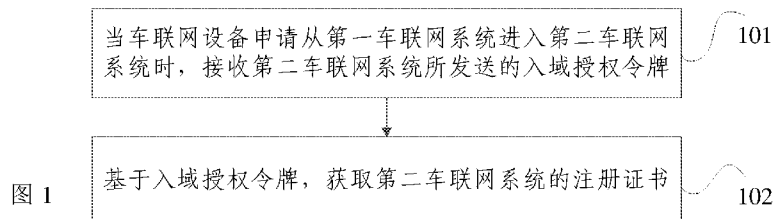
LIMITED); 中国北京市海淀区苏州街29号维亚大厦12层12130室, Beijing 100080 (CN)。

(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, IT, 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, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, 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: METHOD AND APPARATUS FOR APPLYING FOR CERTIFICATE

(54) 发明名称: 一种证书申请方法及装置



101 WHEN AN INTERNET OF VEHICLES DEVICE APPLIES TO ENTER A SECOND INTERNET OF VEHICLES SYSTEM FROM A FIRST INTERNET OF VEHICLES SYSTEM, RECEIVE A DOMAIN ENTRY AUTHORIZATION TOKEN SENT BY THE SECOND INTERNET OF VEHICLES SYSTEM
102 OBTAIN A REGISTRATION CERTIFICATE OF THE SECOND INTERNET OF VEHICLES SYSTEM ON THE BASIS OF THE DOMAIN ENTRY AUTHORIZATION TOKEN

(57) Abstract: Provided in the embodiments of the present disclosure are a method and apparatus for applying for a certificate. The method comprises: when an Internet of Vehicles device applies to enter a second Internet of Vehicles system from a first Internet of Vehicles system, receiving a domain entry authorization token sent by the second Internet of Vehicles system; and obtaining a registration certificate of the second Internet of Vehicles system on the basis of the domain entry authorization token. The embodiments of the present disclosure implement a cross-system certificate application process.

(57) 摘要: 本公开实施例提供一种证书申请方法及装置, 其中方法包括: 当车联网设备申请从第一车联网系统进入第二车联网系统时, 接收所述第二车联网系统所发送的入域授权令牌; 基于所述入域授权令牌, 获取所述第二车联网系统的注册证书。本公开实施例实现了跨系统的证书申请过程。

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))。

一种证书申请方法及装置

相关申请的交叉引用

本申请要求于 2020 年 03 月 18 日提交的申请号为 2020101934358，发明名称为“一种证书申请方法及装置”的中国专利申请的优先权，其通过引用方式全部并入本文。

技术领域

本公开涉及通信技术领域，尤其涉及一种证书申请方法及装置。

背景技术

在车联网安全通信领域，车辆分属于不同的车联网通信系统。当车辆需要跨国行驶时，车辆需要跨系统进入其他国家的车联网系统。另外，即使在同一个国家内，也可能有属于不同车联网通信系统的车辆因某种原因需要进入其他车联网通信系统的场景存在。此时需要考虑到车辆的跨系统进入，但是现有技术并未涉及到。

发明内容

本公开实施例提供一种证书申请方法及装置，以实现车联网设备的跨系统进入过程。

本公开实施例提供一种证书申请方法，应用于车联网设备，包括：

当车联网设备申请从第一车联网系统进入第二车联网系统时，接收所述第二车联网系统所发送的入域授权令牌；

基于所述入域授权令牌，获取所述第二车联网系统的注册证书。

本公开实施例提供一种证书申请方法，应用于第一车联网系统，包括：

当车联网设备申请从第一车联网系统进入第二车联网系统时，接收车联网设备发送的出域申请消息；

基于所述出域申请消息，向所述车联网设备发送出域授权令牌，其中所述出域授权令牌中包含有所述车联网设备的设备签名证书，以使所述车联网

设备向所述第二车联网系统发送入域申请消息并获取入域授权令牌，所述入域申请消息中包含有所述出域授权令牌，且所述入域申请消息通过所述设备签名证书所对应的私钥进行数字签名。

本公开实施例提供一种证书申请方法，应用于第二车联网系统，包括：

- 5 当车联网设备申请从第一车联网系统进入第二车联网系统时，向所述车联网设备发送入域授权令牌，以使所述车联网设备基于所述入域授权令牌获取所述第二车联网系统的注册证书。

本公开实施例提供一种证书申请装置，应用于车联网设备，包括：

- 10 接收模块，用于当车联网设备申请从第一车联网系统进入第二车联网系统时，接收所述第二车联网系统所发送的入域授权令牌；

获取模块，用于基于所述入域授权令牌，获取所述第二车联网系统的注册证书。

本公开实施例提供一种证书申请装置，应用于第一车联网系统，包括：

- 15 接收模块，用于当车联网设备申请从第一车联网系统进入第二车联网系统时，接收车联网设备发送的出域申请消息；

- 20 发送模块，用于基于所述出域申请消息，向所述车联网设备发送出域授权令牌，其中所述出域授权令牌中包含有所述车联网设备的设备签名证书，以使所述车联网设备向所述第二车联网系统发送入域申请消息并获取入域授权令牌，所述入域申请消息中包含有所述出域授权令牌，且所述入域申请消息通过所述设备签名证书所对应的私钥进行数字签名。

本公开实施例提供一种证书申请装置，应用于第二车联网系统，包括：

发送模块，用于当车联网设备申请从第一车联网系统进入第二车联网系统时，向所述车联网设备发送入域授权令牌，以使所述车联网设备基于所述入域授权令牌获取所述第二车联网系统的注册证书。

- 25 本公开实施例提供一种车联网设备，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，所述处理器执行所述程序时实现所述的证书申请方法的步骤。

本公开实施例提供一种第一车联网系统，包括存储器、处理器及存储在

存储器上并可在处理器上运行的计算机程序，所述处理器执行所述程序时实现所述的证书申请方法的步骤。

5 本公开实施例提供一种第二车联网系统，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，所述处理器执行所述程序时实现所述的证书申请方法的步骤。

本公开实施例提供一种非暂态计算机可读存储介质，其上存储有计算机程序，该计算机程序被处理器执行时实现所述的证书申请方法的步骤。

10 本公开实施例提供的证书申请方法及装置，车联网设备在需要从第一车联网系统进入第二车联网系统时通过接收第二车联网系统所发送的入域授权令牌，并通过该入域授权令牌获取第二车联网系统的注册证书，实现了位于第一车联网系统中的车联网设备能够获取第二车联网系统的入域授权令牌和注册证书，从而实现了跨系统的安全通信证书的申请过程，从而能够实现从第一车联网系统至第二车联网系统的跨系统进入。

15 附图说明

为了更清楚地说明本公开实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作一简单地介绍，显而易见地，下面描述中的附图是本公开的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

20 图 1 为本公开实施例中应用于车联网设备的证书申请方法的步骤流程图；

图 2 为本公开实施例中应用于第一车联网系统的证书申请方法的步骤流程图；

图 3 为本公开实施例中应用于第二车联网系统的证书申请方法的步骤流程图；

25 图 4 为本公开实施例中具体实施例的参考架构图；

图 5 为本公开实施例中应用于车联网设备的证书申请装置的模块框图；

图 6 为本公开实施例中应用于第一车联网系统的证书申请装置的模块框图；

图 7 为本公开实施例中应用于第二车联网系统的证书申请装置的模块框图;

图 8 为本公开实施例中车联网设备的结构示意图;

图 9 为本公开实施例中第一车联网系统的结构示意图;

5 图 10 为本公开实施例中第二车联网系统的结构示意图。

具体实施方式

为使本公开实施例的目的、技术方案和优点更加清楚，下面将结合本公开实施例中的附图，对本公开实施例中的技术方案进行清楚、完整地描述，
10 显然，所描述的实施例是本公开一部分实施例，而不是全部的实施例。基于本公开中的实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都属于本公开保护的范围。

为了便于清楚描述本公开实施例的技术方案，在本公开的各实施例中，若采用了“第一”、“第二”等字样对功能和作用基本相同的相同项或相似
15 项进行区分，本领域技术人员可以理解“第一”、“第二”等字样并不对数量和执行次序进行限定。

在车联网领域，车联网安全通信是基于公钥基础设施（Public Key Infrastructure, PKI）实现的，且车联网 PKI 的基本构成也都相同。

其中，车联网系统中证书申请实体包括：车载单元（On Board Unit, OBU）
20 和路侧单元（Road Side Unit, RSU），其中 OBU 为安装在车辆上的通信设备，负责车辆车对外界的信息交换（vehicle to everything, V2X）消息的发送和接收；RSU 安装在在路侧设备上的通信设备，负责路侧设备 V2X 消息的发送和接收。

此外，车联网 PKI 系统中证书颁发实体包括根证书颁发机构（Root
25 Certificate Authority, Root CA）、注册 CA（Enrollment CA, ECA）和应用 CA（Application CA, ACA），根 CA 是车联网安全 PKI 体系的安全锚点，用于向下级子 CA 颁发子 CA 证书；注册 CA 在 OBU 和 RSU 系统的安全初始化（Security Bootstrap）阶段，向这些实体颁发注册证书，OBU 和 RSU 使

用注册证书申请应用证书；应用 CA 向 OBU 和 RSU 颁发其用于对播发的 V2X 消息进行签名的证书。对应的证书种类包括根证书、注册证书和应用证书，其中根证书是根 CA 的自签证书。根证书是一个 PKI 系统证书链的根节点，又称 PKI 系统的信任锚点（trust anchor）；注册证书由注册 CA 颁发给 OBU 和 RSU，注册证书与设备唯一对应，设备使用注册证书从各授权机构获取其他与车联网安全通信相关的应用证书；应用证书是颁发给 OBU 和 RSU 的用于对其播发的消息进行数字签名的证书，例如 OBU 对其播发的车辆行驶状态信息进行数字签名，RSU 对其播发的交通信号灯状态信息进行数字签名。

此外，现有的应用证书颁发过程通常为，OBU/RSU 向注册 CA 申请注册证书，注册 CA 审核后向 OBU/RSU 颁发注册证书；OBU/RSU 利用注册证书向负责某车联网应用领域的应用 CA 申请具体用于对 V2X 消息进行数字签名的应用证书，应用 CA 审核后向 OBU/RSU 颁发应用证书；OBU/RSU 利用应用证书对其播发的 V2X 消息进行数字签名，并将签名消息连同签名证书一同播发出去；接收 V2X 签名消息的 OBU/RSU 首先利用预先存储的应用 CA 证书对消息中的签名证书进行验证，然后利用通过验证的签名证书验证签名消息的有效性。

上述过程虽然能够实现车联网通信，但是并未涉及到跨系统通信，即车联网设备从一个车联网系统进入到另一个车联网系统，在此本公开实施例对如何跨系统通信进行说明。

如图1所示，为本公开实施例中应用于车联网设备的证书申请方法，该方法包括如下步骤：

步骤101：当车联网设备申请从第一车联网系统进入第二车联网系统时，接收第二车联网系统所发送的入域授权令牌。

具体的，车联网设备可以指参与车联网通信的实体，例如安装在车辆上的时隙车辆通信能力的OBU或安装在路侧交通设备上的实现设备通信能力的RSU。

此外，第一车联网系统和第二车联网系统为两个不同的车联网系统，且可以将第一车联网系统当做源域，将第二车联网系统当做目的域，即针对第

二车联网系统而言，入域指从第一车联网系统进入第二车联网系统，针对第一车联网系统而言，出域指从第一车联网系统进入第二车联网系统。当然，针对同一车联网系统中的车联网设备能够使用能够互认的安全通信证书进行车联网安全通信。

- 5 在本步骤中车联网设备初始位于第一车联网系统，此时若车联网设备需要从第一车联网系统进入第二车联网系统，则可以接收第二车联网系统所发送的入域授权令牌。

10 在此需要说明的是，第二车联网系统中可以包括不同的功能实体，以实现对不同功能的划分，例如第二车联网系统中可以包括跨域申请授权实体，该实体用于在一个车联网系统内负责向出域的车联网设备颁发出域授权令牌或者向入域的车联网设备颁发入域授权令牌；即在本步骤中车联网设备可以接收第二车联网系统中的跨域申请授权实体所发送的入域授权令牌。

15 另外，入域授权令牌指车联网系统颁发的允许车联网设备申请本系统中安全通信证书的令牌。当然，该入域授权令牌可以由跨域申请授权实体颁发，且可以使用其私钥对授权信息进行数字签名，以提供令牌数据的完整性、认证性和不可否认性。

步骤102：基于入域授权令牌，获取第二车联网系统的注册证书。

20 在本步骤中，具体的，车联网设备在接收到入域授权令牌之后，可以获取第二车联网系统的注册证书，从而使得能够基于该注册证书进入第二车联网系统，实现了跨系统的安全通信证书的申请过程，从而能够实现从第一车联网系统至第二车联网系统的跨系统进入。

25 这样，本实施例中的车联网设备在需要从第一车联网系统进入第二车联网系统时接收第二车联网系统所发送的入域授权令牌，并通过该入域授权令牌获取第二车联网系统的注册证书，实现了位于第一车联网系统中的车联网设备能够获取第二车联网系统的入域授权令牌和注册证书，从而实现了跨系统的安全通信证书的申请过程，从而能够实现从第一车联网系统至第二车联网系统的跨系统进入。

此外，进一步地，在本实施例中车联网设备在接收第二车联网系统所发

送的入域授权令牌之前，还可以向第一车联网系统发送出域申请消息，并接收第一车联网系统基于出域申请消息所发送的出域授权令牌，其中出域授权令牌中包含有车联网设备的设备签名证书，然后向第二车联网系统发送入域申请消息，其中入域申请消息中包含有出域授权令牌，且入域申请消息通过设备签名证书所对应的私钥进行数字签名。

具体的，车联网设备在需要进入第二车联网系统时，可以先向第一车联网系统发送出域申请消息，当然此时可以向第一车联网系统中的跨域申请授权实体发送出域申请消息，然后第一车联网系统中的跨域申请授权实体可以基于该出域申请消息向车联网设备发送出域授权令牌，从而使得车联网设备能够通过该出域授权令牌向第二车联网系统发送入域申请消息，且获取第二车联网系统基于该入域申请消息所发送的入域授权令牌。

在此需要说明的是，出域授权令牌指第一车联网系统中的跨域授权实体向本系统中的车联网设备颁发的允许其申请其他车联网系统中安全通信证书的令牌。当然，第一车联网系统中的跨域授权实体可以使用其私钥对授权信息进行数字签名，以提供令牌数据的完整性、认证性和不可否认性。

此外，每个车联网系统中还可以维护一可信证书列表，该可信证书列表中存储有其他车联网系统的签名证书（公钥证书）。即其他车联网系统中的跨域申请授权实体可以使用与签名证书对应的私钥来对其颁发的入域授权令牌或出域授权令牌进行数字签名，此时对应的车联网系统中的跨域申请授权实体则可以使用存储在可信证书列表中的证书验证来自于其他车联网系统的入域授权令牌或出域授权令牌。即本实施例中的入域授权令牌和出域授权令牌均为安全令牌。

具体的，出域授权令牌中包含有车联网设备的设备签名证书（即设备签名公钥证书），且入域申请消息通过设备签名证书所对应的私钥进行数字签名。此时当第二车联网系统接收到该入域申请消息时，可以先获取该入域申请消息中的出域授权令牌，并从预先存储的可信证书列表中获取第一车联网系统的签名公钥证书，即可以获取第一车联网系统中跨域申请授权实体的签名公钥证书，从而通过该第一车联网系统的签名公钥证书验证该出域授权令

牌是否有效；此时当验证出域授权令牌有效时，则可以提取出域授权令牌中的车联网设备的设备签名证书，然后使用该设备签名证书对入域申请消息的数字签名进行验证，此时若入域申请消息的数字签名有效，则可以继续提取出域授权令牌中所包含的其他信息。这样使得能够确定每条入域申请消息所对应的车联网设备，且实现了跨系统申请过程中的安全性和有效性。

还需要说明的是，出域授权令牌中还包含有车联网设备的设备信息和/或注册证书申请消息。

即该出域授权令牌中还可以包括车联网设备的设备信息，例如OBU相关信息、车辆相关信息等；另外，该出域授权令牌中还可以包括注册证书申请消息，即此时可以将申请入域授权令牌的过程与申请注册证书的过程合并，当日该注册证书申请消息可以为申请注册证书而生成的密钥对中的公钥。

另外，进一步地，在本实施例中，车联网设备在向第一车联网系统发送出域申请消息之前，还可以向第二车联网系统发送标识申请消息，然后接收第二车联网系统基于标识申请消息所发送的跨域申请标识，其中跨域申请标识与本次进入申请相对应；其中，出域申请消息和出域授权令牌中均包含有跨域申请标识。

具体的，第二车联网系统中还可以包括跨域申请标识生成实体，负责生成车联网设备申请跨系统车联网通信证书过程唯一对应的跨域申请标识。

此外，跨域申请标识为唯一标识车联网设备申请车联网通信系统通信安全证书过程的标识。具体的，该跨域申请标识的生成可采用与密码协议相关的方式生成，也可以是与密码协议无关的方式生成，在此不进行具体限定。与密码协议相关的方式是指跨域申请标识是经将车联网设备的设备信息和/或申请过程相关的信息经密码运算后生成。

具体的，当车联网设备先向第二车联网系统申请跨域申请标识时，此时车联网设备向第一车联网系统发送的出域申请消息以及第一车联网系统颁发的出域授权令牌中均包含有跨域申请标识，即第一车联网系统可以将第二车联网系统生成的跨域申请标识与其生成的出域授权令牌进行绑定。

在上述实施例的基础上，出域授权令牌中还可以包含有车联网设备的设

备信息和/或注册证书申请消息。

另外，在本实施例中，车联网设备在接收第二车联网系统所发送的入域授权令牌时，可以接收第二车联网系统基于入域申请消息所发送的入域响应消息，其中，入域响应消息中包含有入域授权令牌，且入域授权令牌中包含有设备签名证书和与本次进入申请所对应的跨域申请标识。

当然，入域授权令牌中还包含车联网设备的设备信息和/或车联网设备在第二车联网系统中的设备标识。

此外，入域响应消息中还包含有第二车联网系统中注册 CA 的地址信息和/或第二车联网系统中应用 CA 的地址信息。这使得物联网设备能够基于地址信息发送注册证书申请消息以及应用证书申请消息。

另外，在本实施例中，车联网设备在基于入域授权令牌获取第二车联网系统的注册证书时，可以向第二车联网系统发送注册证书申请消息，其中注册证书申请消息中包含有入域授权令牌，且注册证书申请消息通过设备签名证书所对应的私钥进行数字签名，然后接收第二车联网系统基于注册证书申请消息所发送的注册证书。

具体的，第二车联网系统中还可以包括注册 CA，即车联网设备可以向第二车联网系统中的注册 CA 发送注册证书申请消息，以便申请第二车联网系统的注册证书。此时，第二车联网系统中的注册 CA 在接收到注册证书申请消息时，可以获取注册证书申请消息中的入域授权令牌，并获取入域授权令牌中的设备签名证书，然后采用该设备签名证书对注册证书申请消息的数字签名进行验证，并在验证通过后向车联网设备颁发注册证书，从而保证了证书申请过程中的安全性。

当然，车联网设备在基于入域授权令牌获取第二车联网系统的注册证书之后，还可以向第二车联网系统发送应用证书申请消息，其中应用证书申请消息中包含有注册证书，然后接收第二车联网系统基于应用证书申请消息所发送的应用证书。

当然在此需要说明的是，该应用证书申请消息同样可以采用设备签名证书所对应的私钥进行数字签名，过程同注册证书申请过程，在此不再进行具

体说明。

即车联网设备在得到第二车联网系统的注册证书之后，可以利用该第二车联网系统的注册证书向第二车联网系统的应用 CA 申请在第二车联网系统实现车联网安全通信的应用证书，从而实现车联网设备的跨系统安全通信。

5 这样，本实施例中的车联网设备通过接收第二车联网系统所发送的入域授权令牌，并通过该入域授权令牌获取第二车联网系统的注册证书，实现了位于第一车联网系统中的车联网设备能够获取第二车联网系统的入域授权令牌和注册证书，从而实现了跨系统的安全通信证书的申请过程，从而能够实现从第一车联网系统至第二车联网系统的跨系统进入。

10 如图 2 所示，为本公开实施例中应用于第一车联网系统的证书申请方法的步骤流程图，该方法包括如下步骤：

步骤 201：当车联网设备申请从第一车联网系统进入第二车联网系统时，接收车联网设备发送的出域申请消息。

15 具体的，当车联网设备需要进行跨系统通信时，可以先向第一车联网系统发送出域申请消息，此时第一车联网系统接入该出域申请消息。

在此需要说明的是，关于第一车联网系统、第二车联网系统及出域申请消息的具体内容可以参见上述车联网设备侧的相关内容，在此不再进行具体限定。

步骤 202：基于出域申请消息，向车联网设备发出域授权令牌。

20 具体的，第一车联网系统在获取到出域申请消息时，可以向车联网设备发出域授权令牌。

其中，出域授权令牌中包含有车联网设备的设备签名证书，以使车联网设备向第二车联网系统发送入域申请消息并获取入域授权令牌，入域申请消息中包含有出域授权令牌，且入域申请消息通过设备签名证书所对应的私钥进行数字签名。

25 在此需要说明的是，上述内容的相关介绍可以参见上述车联网设备侧的相关内容，在此不再进行具体限定。

此外，需要说明的是，出域申请消息和出域授权令牌中均包含有跨域申

请标识；其中，跨域申请标识为车联网设备向第二车联网系统申请得到，且跨域申请标识与本次进入申请相对应。

当然，还需要补充的是，出域授权令牌中还包含有车联网设备的设备信息和/或注册证书申请消息。

5 在此需要说明的是，上述各项信息的具体内容可以参见车联网设备侧方法实施例的具体相关内容，在此不再进行具体介绍。

这样，本实施例中的第一车联网系统通过接收车联网设备发送的出域申请消息，并基于该出域申请消息向车联网设备发出域授权令牌，使得车联网设备能够基于该出域授权令牌获取第二车联网系统的入域授权令牌，从而
10 实现了跨系统的安全通信证书的申请过程，从而能够实现从第一车联网系统至第二车联网系统的跨系统进入。

此外，如图 3 所示，为本公开实施例中应用于第二车联网系统的证书申请方法的步骤流程图，该方法包括如下步骤：

步骤 301: 当车联网设备申请从第一车联网系统进入第二车联网系统时，
15 向车联网设备发送入域授权令牌。

具体的，当车联网设备需要进行跨域通信时，第二车联网系统可以向车联网设备发送入域授权令牌，从而使得车联网设备能够基于入域授权令牌获取第二车联网系统的注册证书。

具体的，第二车联网系统向车联网设备发送入域授权令牌时，可以接收
20 车联网设备所发送的入域申请消息，其中入域申请消息中包含有出域授权令牌，出域授权令牌由车联网设备向第一车联网系统申请得到，且出域授权令牌中包含有车联网设备的设备签名证书，入域申请消息通过设备签名证书所对应的私钥进行数字签名；然后基于入域申请消息，向车联网设备发送入域响应消息，其中，入域响应消息中包含有入域授权令牌，且入域授权令牌中
25 包含有设备签名证书和与本次进入申请所对应的跨域申请标识。

在此需要说明的是，该实施例中的相关内容可以参见车联网设备侧实施例的相关内容，在此不再进行具体赘述。

此外，进一步地，第二车联网系统在基于入域申请消息，向车联网设备

发送入域响应消息之前，还可以获取入域申请消息中的出域授权令牌，并获取出域授权令牌中的设备签名证书；当通过设备签名证书验证得到入域申请消息的数字签名为有效签名时，确定入域申请消息为有效消息。

即第二车联网系统在向车联网设备颁发入域授权令牌之前，需要验证入域申请消息的有效性，即需要确定申请入域授权令牌的车联网设备的身份信息，此时第二车联网系统可以先从入域申请消息中获取出域授权令牌，并基于预先存储的可信证书列表中第一车联网系统的签名公钥证书验证该出域授权令牌是否有效；当验证得到出域授权令牌有效时则可以获取出域授权令牌中的设备签名证书，从而能够通过该设备签名证书对入域申请消息的数字签名的有效性进行验证；此时，若验证得到入域申请消息的数字签名为有效签名，则可以确定入域申请消息为有效消息，即可以确定车联网设备的身份信息，此时则可以进一步颁发入域授权令牌。

此外，在本实施例中，第二车联网系统在接收车联网设备所发送的入域申请消息之前，还可以接收车联网设备所发送的标识申请消息，并基于标识申请消息，向车联网设备发送跨域申请标识，其中跨域申请标识与本次进入申请相对应。相应地，出域授权令牌中还包含有跨域申请标识。

当然，具体的，出域授权令牌中还包含有车联网设备的设备信息和/或注册证书申请消息。

此外，具体的，入域授权令牌中还包含有车联网设备的设备信息和/或车联网设备在所述第二车联网系统中的设备标识。入域响应消息中还包含有第二车联网系统中注册证书颁发机构 CA 的地址信息；第二车联网系统中应用 CA 的地址信息。

在此需要说明的是，关于上述信息的具体介绍可以参见车联网设备侧实施例的相关内容，在此不再进行具体介绍。

此外，具体的，第二车联网系统在向车联网设备发送入域授权令牌之后，可以接收车联网设备所发送的注册证书申请消息，其中注册证书申请消息中包含有入域授权令牌，且注册证书申请消息通过设备签名证书所对应的私钥进行数字签名；然后获取注册证书申请消息中的入域授权令牌，并获取入域

授权令牌中的设备签名证书，并当通过设备签名证书验证得到注册证书申请消息的数字签名为有效签名时，确定注册证书申请消息为有效消息，并向车联网设备发送注册证书。

当然，第二车联网系统向车联网设备发送注册证书之后，还可以接收车联网设备所发送的应用证书申请消息，其中应用证书申请消息中包含有注册证书；然后基于应用证书申请消息，向车联网设备发送应用证书。

在此需要说明的是，上述过程的具体内容可以参见车联网设备侧实施例的相关内容，在此不再进行赘述。

这样，本实施例中的第二车联网系统通过向车联网设备发送入域授权令牌，实现了跨系统的安全通信证书的申请过程，从而能够实现从第一车联网系统至第二车联网系统的跨系统进入。

下面通过完整的证书申请流程对上述实施例进行具体说明。

参见图 4 所示的框架图，在车联网设备跨系统申请安全通信证书的过程中，假设第一车联网系统中的车联网设备申请第二车联网系统中的安全通信证书，则其中一种申请过程可以包括如下步骤：

1，车联网设备向第二车联网系统中的跨域申请标识生成实体申请跨域申请标识。当然依据第二车联网系统的要求，用于申请跨域申请标识的标识申请消息中还可以包含有与证书申请相关的一些信息，例如车联网设备所在国别、车牌号、进入时间和离开时间等。

此外，跨域申请标识生成实体向车联网设备分配一个与本次申请唯一对应的跨域申请标识，同时还可将该跨域申请标识提供给本系统中的跨域申请授权实体。跨域申请标识的生成可以是基于密码学的方法生成，也可以是不基于密码学的方法生成，在此不做限定。

2，车联网设备向第一车联网系统中的跨域申请授权实体申请出域授权令牌。该出域申请消息中可包含由第二车联网系统中的跨域申请授权实体分配的跨域申请标识。当然依据第一车联网系统的要求，该出域申请消息中可能需提供一些相关信息，例如欲进入的国别、车牌号、车辆类型、车辆用途、进入时间和离开时间等。

3, 第一车联网系统中的跨域申请授权实体检查出域申请消息, 若允许, 则为该车联网设备生成一个出域授权令牌。该出域授权令牌可包含如下信息: 由第二车联网系统中的跨域申请标识生成实体分配的跨域申请标识; 车联网设备的设备签名证书, 车联网设备将使用与该证书对应的私钥对入域申请消息进行数字签名; 车联网设备的设备信息, 例如OBU相关的信息和车辆相关的信息等; 其他信息, 例如令牌颁发者标识、令牌有效期、签名证书信息、进入时间和离开时间等。

4, 车联网设备向第二车联网系统中的跨域申请授权实体申请入域授权令牌, 即发送入域申请消息。该入域申请消息使用与出域授权令牌中包含的设备签名证书相对应的私钥进行数字签名。该入域申请消息中包含有出域授权令牌。

5, 第二车联网系统中的跨域申请授权实体验证该入域申请消息, 具体操作包括: 获取入域申请消息中的出域授权令牌, 从预先存储的可信证书列表中获取第一车联网系统的跨域申请授权实体的签名公钥证书, 然后使用该公钥证书验证出域授权令牌是否有效; 若出域授权令牌有效, 则提取出域授权令牌中的签名公钥证书, 然后使用该证书验证入域申请消息的数字签名是否有效; 若数字签名有效, 则提取令牌中携带的设备和车辆参数, 并利用“域映射策略”将第一车联网系统的参数映射至第二车联网系统, 例如车辆类型、车辆用途, 日期和时间格式等。

6, 第二车联网系统的跨域申请授权实体为车联网设备生成一个入域授权令牌, 其中包含有: 跨域申请标识; 物联网设备的设备签名证书; 第二车联网系统为物联网设备新分配的一个在本系统中使用的设备标识; 已经映射至本系统的物联网设备的设备信息; 其他信息, 例如令牌颁发者标识、令牌有效期、签名证书信息、进入时间和离开时间等; 第二车联网系统通过入域响应消息发送该入域授权令牌, 且入域响应消息还可包含有本系统中注册CA和/或应用CA的地址和所使用的协议等信息。

7, 物联网设备依据第二车联网系统规定的协议向第二车联网系统中的注册CA申请注册证书, 注册证书申请消息使用与入域授权令牌中包含的设备签

名证书相对应的设备签名私钥签名。该注册证书申请消息中可包含入域授权令牌以及物联网设备为申请注册证书而生成的密钥对中的公钥。

8, 第二车联系统注册CA验证注册证书申请消息, 具体操作包括: 注册CA获取注册证书申请消息中的入域授权令牌, 利用第二车联系统中的跨域申请授权实体的公钥证书验证入域授权令牌是否有效, 若令牌有效, 则提取令牌中的物联网设备的设备签名证书, 然后使用该设备签名证书验证注册证书申请消息的数字签名是否有效; 若数字签名有效, 则提取入域授权令牌中的各种设备参数和车辆参数, 以及令牌中提供的公钥等信息为车联设备颁发注册证书。

9, 车联设备利用收到的注册证书, 依据第二车联系统规定的协议向第二车联系统中的应用CA申请相应的应用证书。应用CA验证该应用证书申请消息, 然后依据本系统规则向物联网设备颁发相应应用证书。

10, 物联网设备利用应用证书实现在第二车联系统的车联安全通信。至此, 完成整个证书申请过程。

此外, 另一申请过程还可以为, 物联网设备向第一车联系统的跨域授权实体申请出域授权令牌, 后者向物联网设备颁发出域授权令牌, 令牌中包含有设备签名证书; 然后, 物联网设备将备出域授权令牌提供给第二车联系统的跨域授权实体, 后者首先生成跨域申请标识, 然后向物联网设备颁发入域授权令牌, 颁发的令牌中包含有跨域申请标识和设备签名证书; 再然后, 物联网设备利用入域授权令牌申请第二车联系统的注册证书和应用证书。

此外, 另一申请过程还可以为, 申请入域授权令牌的过程与申请注册证书的过程合并, 即出域授权令牌中还可以包含注册证书申请消息。

此外, 如图5所示, 为本公开实施例中应用于车联设备的证书申请装置的模块框图, 该装置包括:

接收模块 501, 用于当车联设备申请从第一车联系统进入第二车联系统时, 接收所述第二车联系统所发送的入域授权令牌;

获取模块 502, 用于基于所述入域授权令牌, 获取所述第二车联系统的注册证书。

可选地，装置还包括：

第一发送模块，用于向所述第一车联网系统发送出域申请消息；

第一接收单元，用于接收所述第一车联网系统基于所述出域申请消息所发送的出域授权令牌，其中所述出域授权令牌中包含有所述车联网设备的设备签名证书；

第二发送模块，用于向所述第二车联网系统发送入域申请消息，其中所述入域申请消息中包含有所述出域授权令牌，且所述入域申请消息通过所述设备签名证书所对应的私钥进行数字签名。

在此需要说明的是，该装置能够实现车联网设备方法实施例侧的所有方法步骤，并能够达到相同的技术效果，在此不再进行赘述。

如图6所示，为本公开实施例中应用于第一车联网系统的证书申请装置的模块框图，该装置包括：

接收模块 601，用于当车联网设备申请从第一车联网系统进入第二车联网系统时，接收车联网设备发送的出域申请消息；

发送模块 602，用于基于所述出域申请消息，向所述车联网设备发送出域授权令牌，其中所述出域授权令牌中包含有所述车联网设备的设备签名证书，以使所述车联网设备向所述第二车联网系统发送入域申请消息并获取入域授权令牌，所述入域申请消息中包含有所述出域授权令牌，且所述入域申请消息通过所述设备签名证书所对应的私钥进行数字签名。

可选地，所述出域申请消息和所述出域授权令牌中均包含有跨域申请标识；其中，所述跨域申请标识为所述车联网设备向所述第二车联网系统申请得到，且所述跨域申请标识与本次进入申请相对应。

在此需要说明的是，该装置能够实现第一车联网系统方法实施例侧的所有方法步骤，并能够达到相同的技术效果，在此不再进行赘述。

如图7所示，为本公开实施例中应用于第二车联网系统的证书申请装置的模块框图，该装置包括：

发送模块 701，用于当车联网设备申请从第一车联网系统进入第二车联网系统时，向所述车联网设备发送入域授权令牌，以使所述车联网设备基于

所述入域授权令牌获取所述第二车联网系统的注册证书。

5 可选地，发送模块 701 具体用于，接收所述车联网设备所发送的入域申请消息，其中所述入域申请消息中包含有出域授权令牌，所述出域授权令牌由所述车联网设备向所述第一车联网系统申请得到，且所述出域授权令牌中包含有所述车联网设备的设备签名证书，所述入域申请消息通过所述设备签名证书所对应的私钥进行数字签名；基于所述入域申请消息，向所述车联网设备发送入域响应消息，其中，所述入域响应消息中包含有入域授权令牌，且所述入域授权令牌中包含有所述设备签名证书和与本次进入申请所对应的跨域申请标识，所述入域响应消息通过所述设备签名证书所对应的私钥进行数字签名。

10

在此需要说明的是，该装置能够实现第二车联网系统方法实施例侧的所有方法步骤，并能够达到相同的技术效果，在此不再进行赘述。

图 8 为本公开一实施例提供的车联网设备的结构示意图，如图 8 所示，该车联网设备 800 可以包括至少一个处理器 801、存储器 802、至少一个其他的用户接口 803，以及收发机 804。车联网设备 800 中的各个组件通过总线系统 805 耦合在一起。可理解，总线系统 805 用于实现这些组件之间的连接通信。总线系统 805 除包括数据总线之外，还包括电源总线、控制总线和状态信号总线。但是为了清楚说明起见，在图 8 中将各种总线都标为总线系统 805，总线系统可以包括任意数量的互联的总线和桥，具体由处理器 801 代表的一个或多个处理器和存储器 802 代表的存储器的各种电路链接在一起。总线系统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，本公开实施例不再对其进行进一步描述。总线接口提供接口。收发机 804 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 803 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。

15

20

25

可以理解，本公开实施例中的存储器 802 可以是易失性存储器或非易失性存储器，或可包括易失性和非易失性存储器两者。其中，非易失性存储器

可以是只读存储器(Read-Only Memory, ROM)、可编程只读存储器(Programmable ROM, PROM)、可擦除可编程只读存储器(Erasable PROM, EPROM)、电可擦除可编程只读存储器(Electrically EPROM, EEPROM)或闪存。易失性存储器可以是随机存取存储器(Random Access Memory, RAM),
5 其用作外部高速缓存。通过示例性但不是限制性说明,许多形式的RAM可用,例如静态随机存取存储器(Static RAM, SRAM)、动态随机存取存储器(Dynamic RAM, DRAM)、同步动态随机存取存储器(Synchronous DRAM, SDRAM)、双倍数据速率同步动态随机存取存储器(Double Data Rate SDRAM, DDRSDRAM)、增强型同步动态随机存取存储器(Enhanced SDRAM, ESDRAM)、同步连接动态随机存取存储器(Synchlink DRAM, SLDRAM)和直接内存总线随机存取存储器(Direct Rambus RAM, DRRAM)。本公开各实施例所描述的系统和方法的存储器802旨在包括但不限于这些和任意其它适合类型的存储器。

处理器801负责管理总线系统和通常的处理,存储器802可以存储处理
15 器801在执行操作时所使用的计算机程序或指令,具体地,处理器801可以用于:当车联网设备申请从第一车联网系统进入第二车联网系统时,接收所述第二车联网系统所发送的入域授权令牌;基于所述入域授权令牌,获取所述第二车联网系统的注册证书。

上述本公开实施例揭示的方法可以应用于处理器801中,或者由处理器
20 801实现。处理器801可能是一种集成电路芯片,具有信号的处理能力。在实现过程中,上述方法的各步骤可以通过处理器801中的硬件的集成逻辑电路或者软件形式的指令完成。上述的处理器801可以是通用处理器、数字信号处理器(Digital Signal Processor, DSP)、专用集成电路(Application Specific Integrated Circuit, ASIC)、现成可编程门阵列(Field Programmable Gate Array, FPGA)或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件。可以实现或者执行本公开实施例中的公开的各方法、步骤及逻辑框图。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。结合本公开实施例所公开的方法的步骤可以直接体现为硬件译码处理器执行完

成，或者用译码处理器中的硬件及软件模块组合执行完成。软件模块可以位于随机存储器，闪存、只读存储器，可编程只读存储器或者电可擦写可编程存储器、寄存器等本领域成熟的存储介质中。该存储介质位于存储器 802，处理器 801 读取存储器 802 中的信息，结合其硬件完成上述方法的步骤。

5 可以理解的是，本公开描述的这些实施例可以用硬件、软件、固件、中间件、微码或其组合来实现。对于硬件实现，处理单元可以实现在一个或多个专用集成电路(Application Specific Integrated Circuits, ASIC)、数字信号处理器(Digital Signal Processing, DSP)、数字信号处理设备(DSP Device, DSPD)、可编程逻辑设备(Programmable Logic Device, PLD)、现场可编程门阵列
10 (Field-Programmable Gate Array, FPGA)、通用处理器、控制器、微控制器、微处理器、用于执行本申请所述功能的其它电子单元或其组合中。

对于软件实现，可通过执行本公开实施例中所述功能的模块(例如过程、函数等)来实现所述的技术。软件代码可存储在存储器中并通过处理器执行。存储器可以在处理器中或在处理器外部实现。

15 可选地，作为另一个实施例，所述接收所述第二车联网系统所发送的入域授权令牌之前，处理器 801 还用于：向所述第一车联网系统发送出域申请消息；接收所述第一车联网系统基于所述出域申请消息所发送的出域授权令牌，其中所述出域授权令牌中包含有所述车联网设备的设备签名证书；向所述
20 所述第二车联网系统发送入域申请消息，其中所述入域申请消息中包含有所说出域授权令牌，且所述入域申请消息通过所述设备签名证书所对应的私钥进行数字签名。

可选地，作为另一个实施例，所述向所述第一车联网系统发送出域申请消息之前，处理器 801 还用于：向所述第二车联网系统发送标识申请消息；接收所述第二车联网系统基于所述标识申请消息所发送的跨域申请标识，其中
25 所述跨域申请标识与本次进入申请相对应；其中，所述出域申请消息和所述出域授权令牌中均包含有所述跨域申请标识。

可选地，作为另一个实施例，所述出域授权令牌中还包含有所述车联网设备的设备信息和/或注册证书申请消息。

可选地，作为另一个实施例，处理器 801 还用于：接收所述第二车联网系统基于所述入域申请消息所发送的入域响应消息，其中，所述入域响应消息中包含有所述入域授权令牌，且所述入域授权令牌中包含有所述设备签名证书和与本次进入申请所对应的跨域申请标识。

5 可选地，作为另一个实施例，所述入域授权令牌中还包含所述车联网设备的设备信息和/或所述车联网设备在所述第二车联网系统中的设备标识；所述入域响应消息中还包含有所述第二车联网系统中注册证书颁发机构 CA 的地址信息和/或所述第二车联网系统中应用 CA 的地址信息。

10 可选地，作为另一个实施例，处理器 801 还用于：向所述第二车联网系统发送注册证书申请消息，其中所述注册证书申请消息中包含有所述入域授权令牌，且所述注册证书申请消息通过所述设备签名证书所对应的私钥进行数字签名；接收所述第二车联网系统基于所述注册证书申请消息所发送的注册证书。

15 可选地，作为另一个实施例，处理器 801 还用于：向所述第二车联网系统发送应用证书申请消息，其中所述应用证书申请消息中包含有所述注册证书；接收所述第二车联网系统基于所述应用证书申请消息所发送的应用证书。

本公开实施例提供的车联网设备能够实现前述实施例中车联网设备实现的各个过程，为避免重复，此处不再赘述。

20 图 9 为本公开一实施例提供的第一车联网系统的结构示意图，如图 9 所示，该第一车联网系统 900 可以包括至少一个处理器 901、存储器 902、至少一个其他的用户接口 903，以及收发机 904。第一车联网系统 900 中的各个组件通过总线系统 905 耦合在一起。可理解，总线系统 905 用于实现这些组件之间的连接通信。总线系统 905 除包括数据总线之外，还包括电源总线、控制总线和状态信号总线。但是为了清楚说明起见，在图 9 中将各种总线都标为总线系统 905，总线系统可以包括任意数量的互联的总线和桥，具体由处理器 901 代表的一个或多个处理器和存储器 902 代表的存储器的各种电路链接在一起。总线系统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，本公开实施

例不再对其进行进一步描述。总线接口提供接口。收发机 904 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 903 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。

可以理解，本公开实施例中的存储器 902 可以是易失性存储器或非易失性存储器，或可包括易失性和非易失性存储器两者。其中，非易失性存储器可以是只读存储器 (Read-Only Memory, ROM)、可编程只读存储器 (Programmable ROM, PROM)、可擦除可编程只读存储器 (Erasable PROM, EPROM)、电可擦除可编程只读存储器 (Electrically EPROM, EEPROM) 或闪存。易失性存储器可以是随机存取存储器 (Random Access Memory, RAM)，其用作外部高速缓存。通过示例性但不是限制性说明，许多形式的 RAM 可用，例如静态随机存取存储器 (Static RAM, SRAM)、动态随机存取存储器 (Dynamic RAM, DRAM)、同步动态随机存取存储器 (Synchronous DRAM, SDRAM)、双倍数据速率同步动态随机存取存储器 (Double Data Rate SDRAM, DDRSDRAM)、增强型同步动态随机存取存储器 (Enhanced SDRAM, ESDRAM)、同步连接动态随机存取存储器 (Synchlink DRAM, SLDRAM) 和直接内存总线随机存取存储器 (Direct Rambus RAM, DRRAM)。本公开各实施例所描述的系统和方法的存储器 902 旨在包括但不限于这些和任意其它适合类型的存储器。

处理器 901 负责管理总线系统和通常的处理，存储器 902 可以存储处理器 901 在执行操作时所使用的计算机程序或指令，具体地，处理器 901 可以用于：当车联网设备申请从第一车联网系统进入第二车联网系统时，接收车联网设备发送的出域申请消息；基于所述出域申请消息，向所述车联网设备发出域授权令牌，其中所述出域授权令牌中包含有所述车联网设备的设备签名证书，以使所述车联网设备向所述第二车联网系统发送入域申请消息并获取入域授权令牌，所述入域申请消息中包含有所述出域授权令牌，且所述入域申请消息通过所述设备签名证书所对应的私钥进行数字签名。

可选地，作为另一个实施例，所述出域申请消息和所述出域授权令牌中均包含有跨域申请标识；其中，所述跨域申请标识为所述车联网设备向所述第二车联网系统申请得到，且所述跨域申请标识与本次进入申请相对应。

5 可选地，作为另一个实施例，所述出域授权令牌中还包含有所述车联网设备的设备信息和/或注册证书申请消息。

本公开实施例提供的第一车联网系统能够实现前述实施例中第一车联网系统实现的各个过程，为避免重复，此处不再赘述。

图 10 为本公开一实施例提供的第二车联网系统的结构示意图，如图 10 所示，该第二车联网系统 1000 可以包括至少一个处理器 1001、存储器 1002、
10 至少一个其他的用户接口 1003，以及收发机 1004。第二车联网系统 1000 中的各个组件通过总线系统 1005 耦合在一起。可理解，总线系统 1005 用于实现这些组件之间的连接通信。总线系统 1005 除包括数据总线之外，还包括电源总线、控制总线和状态信号总线。但是为了清楚说明起见，在图 10 中将各种总线都标为总线系统 1005，总线系统可以包括任意数量的互联的总线和桥，
15 具体由处理器 1001 代表的一个或多个处理器和存储器 1002 代表的存储器的各种电路链接在一起。总线系统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，本公开实施例不再对其进行进一步描述。总线接口提供接口。收发机 1004
20 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 1003 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。

可以理解，本公开实施例中的存储器 1002 可以是易失性存储器或非易失性存储器，或可包括易失性和非易失性存储器两者。其中，非易失性存储器
25 可以是只读存储器(Read-Only Memory, ROM)、可编程只读存储器(Programmable ROM, PROM)、可擦除可编程只读存储器(Erasable PROM, EPROM)、电可擦除可编程只读存储器(Electrically EPROM, EEPROM)或闪存。易失性存储器可以是随机存取存储器(Random Access Memory, RAM)，

其用作外部高速缓存。通过示例性但不是限制性说明，许多形式的 RAM 可用，例如静态随机存取存储器(Static RAM, SRAM)、动态随机存取存储器(Dynamic RAM, DRAM)、同步动态随机存取存储器(Synchronous DRAM, SDRAM)、双倍数据速率同步动态随机存取存储器(Double Data Rate SDRAM, DDRSDRAM)、增强型同步动态随机存取存储器(Enhanced SDRAM, ESDRAM)、同步连接动态随机存取存储器(Synchlink DRAM, SLDRAM)和直接内存总线随机存取存储器(Direct Rambus RAM, DRRAM)。本公开各实施例所描述的系统和方法的存储器 1002 旨在包括但不限于这些和任意其它适合类型的存储器。

10 处理器 1001 负责管理总线系统和通常的处理，存储器 1002 可以存储处理器 1001 在执行操作时所使用的计算机程序或指令，具体地，处理器 1001 可以用于：当车联网设备申请从第一车联网系统进入第二车联网系统时，向所述车联网设备发送入域授权令牌，以使所述车联网设备基于所述入域授权令牌获取所述第二车联网系统的注册证书。

15 可选地，作为另一个实施例，处理器 1001 还用于：接收所述车联网设备所发送的入域申请消息，其中所述入域申请消息中包含有出域授权令牌，所述出域授权令牌由所述车联网设备向所述第一车联网系统申请得到，且所述出域授权令牌中包含有所述车联网设备的设备签名证书，所述入域申请消息通过所述设备签名证书所对应的私钥进行数字签名；基于所述入域申请消息，
20 向所述车联网设备发送入域响应消息，其中，所述入域响应消息中包含有入域授权令牌，且所述入域授权令牌中包含有所述设备签名证书和与本次进入申请所对应的跨域申请标识。

可选地，作为另一个实施例，所述接收所述车联网设备所发送的入域申请消息之前，处理器 1001 还用于：接收所述车联网设备所发送的标识申请消息；基于所述标识申请消息，向所述车联网设备发送跨域申请标识，其中所述跨域申请标识与本次进入申请相对应；相应地，所述出域授权令牌中还包含有所述跨域申请标识。

可选地，作为另一个实施例，所述出域授权令牌中还包含有所述车联网

设备的设备信息和/或注册证书申请消息。

可选地，作为另一个实施例，所述入域授权令牌中还包含有所述车联网设备的设备信息和/或所述车联网设备在所述第二车联网系统中的设备标识；所述入域响应消息中还包含有所述第二车联网系统中注册证书颁发机构 CA 的地址信息和/或所述第二车联网系统中应用 CA 的地址信息。

可选地，作为另一个实施例，所述基于所述入域申请消息，向所述车联网设备发送入域响应消息之前，处理器 1001 还用于：获取所述入域申请消息中的出域授权令牌，并获取所述出域授权令牌中的设备签名证书；当通过所述设备签名证书验证得到所述入域申请消息的数字签名为有效签名时，确定所述入域申请消息为有效消息。

可选地，作为另一个实施例，所述向所述车联网设备发送入域授权令牌之后，处理器 1001 还用于：接收所述车联网设备所发送的注册证书申请消息，其中所述注册证书申请消息中包含有所述入域授权令牌，且所述注册证书申请消息通过所述设备签名证书所对应的私钥进行数字签名；获取所述注册证书申请消息中的所述入域授权令牌，并获取所述入域授权令牌中的设备签名证书；当通过所述设备签名证书验证得到所述注册证书申请消息的数字签名为有效签名时，确定所述注册证书申请消息为有效消息，并向所述车联网设备发送注册证书。

可选地，作为另一个实施例，所述向所述车联网设备发送注册证书之后，处理器 1001 还用于：接收所述车联网设备所发送的应用证书申请消息，其中所述应用证书申请消息中包含有所述注册证书；基于所述应用证书申请消息，向所述车联网设备发送应用证书。

本公开实施例提供的第二车联网系统能够实现前述实施例中第二车联网系统实现的各个过程，为避免重复，此处不再赘述。

上述主要从电子设备的角度对本公开实施例提供的方案进行了介绍。可以理解的是，本公开实施例提供的电子设备为了实现上述功能，其包含了执行各个功能相应的硬件结构和/或软件模块。本领域技术人员应该很容易意识到，结合本公开中所公开的实施例描述的各示例的单元及算法步骤，本公开

能够以硬件或硬件和计算机软件的结合形式来实现。

某个功能究竟以硬件还是计算机软件驱动硬件的方式来执行，取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能，但是这种实现不应认为超出本公开的范围。

本公开实施例可以根据上述方法示例对电子设备等进行功能模块的划分，例如，可以对应各个功能划分各个功能模块，也可以将两个或两个以上的功能集成在一个处理模块中。上述集成的模块既可以采用硬件的形式实现，也可以采用软件功能模块的形式实现。

需要说明的是，本公开实施例中对模块的划分是示意性的，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。

所属领域的技术人员可以清楚地了解到，为描述的方便和简洁，仅以上述各功能模块的划分进行举例说明，实际应用中，可以根据需要而将上述功能分配由不同的功能模块完成，即将装置的内部结构划分成不同的功能模块，以完成以上描述的全部或者部分功能。上述描述的系统，装置和单元的具体工作过程，可以参考前述方法实施例中的对应过程，在此不再赘述。

在本公开所提供的几个实施例中，应该理解到，所揭露的装置和方法，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，所述模块或单元的划分，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。

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，在本公开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取存储介质中。基于这样的理解，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)或处理器执行本公开各个实施例所述方法的全部或部分步骤。所述计算机存储介质是非短暂性(英文：nontransitory)介质，包括：快闪存储器、移动硬盘、只读存储器、随机存取存储器、磁碟或者光盘等各种可以存储程序代码的介质。

另一方面，本公开实施例还提供一种非暂态计算机可读存储介质，其上存储有计算机程序，该计算机程序被处理器执行时实现上述各实施例提供的方法步骤，并能够达到相同的技术效果，在此不再进行赘述。

最后应说明的是：以上实施例仅用以说明本公开的技术方案，而非对其限制；尽管参照前述实施例对本公开进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本公开各实施例技术方案的精神和范围。

权利要求书

1、一种证书申请方法，应用于车联网设备，其特征在于，包括：

当车联网设备申请从第一车联网系统进入第二车联网系统时，接收所述第二车联网系统所发送的入域授权令牌；

5 基于所述入域授权令牌，获取所述第二车联网系统的注册证书。

2、根据权利要求1所述的证书申请方法，其特征在于，所述接收所述第二车联网系统所发送的入域授权令牌之前，还包括：

向所述第一车联网系统发送出域申请消息；

10 接收所述第一车联网系统基于所述出域申请消息所发送的出域授权令牌，其中所述出域授权令牌中包含有所述车联网设备的设备签名证书；

向所述第二车联网系统发送入域申请消息，其中所述入域申请消息中包含有所述出域授权令牌，且所述入域申请消息通过所述设备签名证书所对应的私钥进行数字签名。

15 3、根据权利要求2所述的证书申请方法，其特征在于，所述向所述第一车联网系统发送出域申请消息之前，还包括：

向所述第二车联网系统发送标识申请消息；

接收所述第二车联网系统基于所述标识申请消息所发送的跨域申请标识，其中所述跨域申请标识与本次进入申请相对应；

20 其中，所述出域申请消息和所述出域授权令牌中均包含有所述跨域申请标识。

4、根据权利要求2或3所述的证书申请方法，其特征在于，所述出域授权令牌中还包含有所述车联网设备的设备信息和/或注册证书申请消息。

5、根据权利要求2所述的证书申请方法，其特征在于，所述接收所述第二车联网系统所发送的入域授权令牌，包括：

25 接收所述第二车联网系统基于所述入域申请消息所发送的入域响应消息，其中，所述入域响应消息中包含有所述入域授权令牌，且所述入域授权令牌中包含有所述设备签名证书和与本次进入申请所对应的跨域申请标识。

6、根据权利要求5所述的证书申请方法，其特征在于，所述入域授权令

牌中还包含有所述车联网设备的设备信息和/或所述车联网设备在所述第二车联网系统中的设备标识；

所述入域响应消息中还包含有所述第二车联网系统中注册证书颁发机构 CA 的地址信息和/或所述第二车联网系统中应用 CA 的地址信息。

- 5 7、根据权利要求 5 所述的证书申请方法，其特征在于，所述基于所述入域授权令牌，获取所述第二车联网系统的注册证书，包括：

向所述第二车联网系统发送注册证书申请消息，其中所述注册证书申请消息中包含有所述入域授权令牌，且所述注册证书申请消息通过所述设备签名证书所对应的私钥进行数字签名；

- 10 接收所述第二车联网系统基于所述注册证书申请消息所发送的注册证书。

8、根据权利要求 1 或 7 所述的证书申请方法，其特征在于，所述基于所述入域授权令牌，获取所述第二车联网系统的注册证书之后，还包括：

向所述第二车联网系统发送应用证书申请消息，其中所述应用证书申请消息中包含有所述注册证书；

- 15 接收所述第二车联网系统基于所述应用证书申请消息所发送的应用证书。

9、一种证书申请方法，应用于第一车联网系统，其特征在于，包括：

当车联网设备申请从第一车联网系统进入第二车联网系统时，接收车联网设备发送的出域申请消息；

- 20 基于所述出域申请消息，向所述车联网设备发出域授权令牌，其中所述出域授权令牌中包含有所述车联网设备的设备签名证书，以使所述车联网设备向所述第二车联网系统发送入域申请消息并获取入域授权令牌，所述入域申请消息中包含有所述出域授权令牌，且所述入域申请消息通过所述设备签名证书所对应的私钥进行数字签名。

- 25 10、根据权利要求 9 所述的证书申请方法，其特征在于，所述出域申请消息和所述出域授权令牌中均包含有跨域申请标识；其中，所述跨域申请标识为所述车联网设备向所述第二车联网系统申请得到，且所述跨域申请标识与本次进入申请相对应。

11、根据权利要求 9 或 10 所述的证书申请方法，其特征在于，所述出域

授权令牌中还包含有所述车联网设备的设备信息和/或注册证书申请消息。

12、一种证书申请方法，应用于第二车联网系统，其特征在于，包括：

当车联网设备申请从第一车联网系统进入第二车联网系统时，向所述车联网设备发送入域授权令牌，以使所述车联网设备基于所述入域授权令牌获取所述第二车联网系统的注册证书。

13、根据权利要求 12 所述的证书申请方法，其特征在于，所述向所述车联网设备发送入域授权令牌，包括：

接收所述车联网设备所发送的入域申请消息，其中所述入域申请消息中包含有出域授权令牌，所述出域授权令牌由所述车联网设备向所述第一车联网系统申请得到，且所述出域授权令牌中包含有所述车联网设备的设备签名证书，所述入域申请消息通过所述设备签名证书所对应的私钥进行数字签名；

基于所述入域申请消息，向所述车联网设备发送入域响应消息，其中，所述入域响应消息中包含有入域授权令牌，且所述入域授权令牌中包含有所述设备签名证书和与本次进入申请所对应的跨域申请标识。

14、根据权利要求 13 所述的证书申请方法，其特征在于，所述接收所述车联网设备所发送的入域申请消息之前，还包括：

接收所述车联网设备所发送的标识申请消息；

基于所述标识申请消息，向所述车联网设备发送跨域申请标识，其中所述跨域申请标识与本次进入申请相对应；

相应地，所述出域授权令牌中还包含有所述跨域申请标识。

15、根据权利要求 13 或 14 所述的证书申请方法，其特征在于，所述出域授权令牌中还包含有所述车联网设备的设备信息和/或注册证书申请消息。

16、根据权利要求 13 所述的证书申请方法，其特征在于，所述入域授权令牌中还包含有所述车联网设备的设备信息和/或所述车联网设备在所述第二车联网系统中的设备标识；

所述入域响应消息中还包含有所述第二车联网系统中注册证书颁发机构 CA 的地址信息和/或所述第二车联网系统中应用 CA 的地址信息。

17、根据权利要求 13 所述的证书申请方法，其特征在于，所述基于所述

入域申请消息，向所述车联网设备发送入域响应消息之前，还包括：

获取所述入域申请消息中的出域授权令牌，并获取所述出域授权令牌中的设备签名证书；

5 当通过所述设备签名证书验证得到所述入域申请消息的数字签名为有效签名时，确定所述入域申请消息为有效消息。

18、根据权利要求 13 所述的证书申请方法，其特征在于，所述向所述车联网设备发送入域授权令牌之后，还包括：

10 接收所述车联网设备所发送的注册证书申请消息，其中所述注册证书申请消息中包含有所述入域授权令牌，且所述注册证书申请消息通过所述设备签名证书所对应的私钥进行数字签名；

获取所述注册证书申请消息中的所述入域授权令牌，并获取所述入域授权令牌中的设备签名证书；

15 当通过所述设备签名证书验证得到所述注册证书申请消息的数字签名为有效签名时，确定所述注册证书申请消息为有效消息，并向所述车联网设备发送注册证书。

19、根据权利要求 18 所述的证书申请方法，其特征在于，所述向所述车联网设备发送注册证书之后，还包括：

接收所述车联网设备所发送的应用证书申请消息，其中所述应用证书申请消息中包含有所述注册证书；

20 基于所述应用证书申请消息，向所述车联网设备发送应用证书。

20、一种证书申请装置，应用于车联网设备，其特征在于，包括：

接收模块，用于当车联网设备申请从第一车联网系统进入第二车联网系统时，接收所述第二车联网系统所发送的入域授权令牌；

25 获取模块，用于基于所述入域授权令牌，获取所述第二车联网系统的注册证书。

21、根据权利要求 20 所述的证书申请装置，其特征在于，在所述接收模块之前，所述证书申请装置还包括：

第一发送模块，用于向所述第一车联网系统发送出域申请消息；

第一接收单元，用于接收所述第一车联网系统基于所述出域申请消息所发送的出域授权令牌，其中所述出域授权令牌中包含有所述车联网设备的设备签名证书；

5 第二发送模块，用于向所述第二车联网系统发送入域申请消息，其中所述入域申请消息中包含有所述出域授权令牌，且所述入域申请消息通过所述设备签名证书所对应的私钥进行数字签名。

22、根据权利要求 21 所述的证书申请装置，其特征在于，在所述第一发送模块之前，所述证书申请装置还包括：

第三发送模块，用于向所述第二车联网系统发送标识申请消息；

10 第二接收单元，用于接收所述第二车联网系统基于所述标识申请消息所发送的跨域申请标识，其中所述跨域申请标识与本次进入申请相对应；

其中，所述出域申请消息和所述出域授权令牌中均包含有所述跨域申请标识。

15 23、根据权利要求 21 或 22 所述的证书申请装置，其特征在于，所述出域授权令牌中还包含有所述车联网设备的设备信息和/或注册证书申请消息。

24、根据权利要求 21 所述的证书申请装置，其特征在于，所述接收模块具体用于：

20 接收所述第二车联网系统基于所述入域申请消息所发送的入域响应消息，其中，所述入域响应消息中包含有所述入域授权令牌，且所述入域授权令牌中包含有所述设备签名证书和与本次进入申请所对应的跨域申请标识。

25、根据权利要求 24 所述的证书申请装置，其特征在于，所述入域授权令牌中还包含有所述车联网设备的设备信息和/或所述车联网设备在所述第二车联网系统中的设备标识；

25 所述入域响应消息中还包含有所述第二车联网系统中注册证书颁发机构 CA 的地址信息和/或所述第二车联网系统中应用 CA 的地址信息。

26、根据权利要求 24 所述的证书申请装置，其特征在于，所述获取模块包括：

发送子模块，用于向所述第二车联网系统发送注册证书申请消息，其中

所述注册证书申请消息中包含有所述入域授权令牌，且所述注册证书申请消息通过所述设备签名证书所对应的私钥进行数字签名；

接收子模块，用于接收所述第二车联网系统基于所述注册证书申请消息所发送的注册证书。

- 5 27、根据权利要求 20 或 26 所述的证书申请装置，其特征在于，所述获取模块之后，所述证书申请装置还包括：

第四发送模块，用于向所述第二车联网系统发送应用证书申请消息，其中所述应用证书申请消息中包含有所述注册证书；

- 10 第三接收单元，用于接收所述第二车联网系统基于所述应用证书申请消息所发送的应用证书。

28、一种证书申请装置，应用于第一车联网系统，其特征在于，包括：

接收模块，用于当车联网设备申请从第一车联网系统进入第二车联网系统时，接收车联网设备发送的出域申请消息；

- 15 发送模块，用于基于所述出域申请消息，向所述车联网设备发送出域授权令牌，其中所述出域授权令牌中包含有所述车联网设备的设备签名证书，以使所述车联网设备向所述第二车联网系统发送入域申请消息并获取入域授权令牌，所述入域申请消息中包含有所述出域授权令牌，且所述入域申请消息通过所述设备签名证书所对应的私钥进行数字签名。

- 20 29、根据权利要求 28 所述的证书申请装置，其特征在于，所述出域申请消息和所述出域授权令牌中均包含有跨域申请标识；其中，所述跨域申请标识为所述车联网设备向所述第二车联网系统申请得到，且所述跨域申请标识与本次进入申请相对应。

30、根据权利要求 28 或 29 所述的证书申请装置，其特征在于，所述出域授权令牌中还包含有所述车联网设备的设备信息和/或注册证书申请消息。

- 25 31、一种证书申请装置，应用于第二车联网系统，其特征在于，包括：

发送模块，用于当车联网设备申请从第一车联网系统进入第二车联网系统时，向所述车联网设备发送入域授权令牌，以使所述车联网设备基于所述入域授权令牌获取所述第二车联网系统的注册证书。

32、根据权利要求 31 所述的证书申请装置，其特征在于，所述发送模块包括：

第一接收子模块，用于接收所述车联网设备所发送的入域申请消息，其中所述入域申请消息中包含有出域授权令牌，所述出域授权令牌由所述车联网设备向所述第一车联网系统申请得到，且所述出域授权令牌中包含有所述车联网设备的设备签名证书，所述入域申请消息通过所述设备签名证书所对应的私钥进行数字签名；

第一发送子模块，用于基于所述入域申请消息，向所述车联网设备发送入域响应消息，其中，所述入域响应消息中包含有入域授权令牌，且所述入域授权令牌中包含有所述设备签名证书和与本次进入申请所对应的跨域申请标识。

33、根据权利要求 32 所述的证书申请装置，其特征在于，所述第一接收子模块之前，还包括：

第二接收子模块，用于接收所述车联网设备所发送的标识申请消息；

第二发送子模块，用于基于所述标识申请消息，向所述车联网设备发送跨域申请标识，其中所述跨域申请标识与本次进入申请相对应；

相应地，所述出域授权令牌中还包含有所述跨域申请标识。

34、根据权利要求 32 或 33 所述的证书申请装置，其特征在于，所述出域授权令牌中还包含有所述车联网设备的设备信息和/或注册证书申请消息。

35、根据权利要求 32 所述的证书申请装置，其特征在于，所述入域授权令牌中还包含有所述车联网设备的设备信息和/或所述车联网设备在所述第二车联网系统中的设备标识；

所述入域响应消息中还包含有所述第二车联网系统中注册证书颁发机构 CA 的地址信息和/或所述第二车联网系统中应用 CA 的地址信息。

36、根据权利要求 32 所述的证书申请装置，其特征在于，所述第一发送子模块之前，还包括：

获取子模块，用于获取所述入域申请消息中的出域授权令牌，并获取所述出域授权令牌中的设备签名证书；

确定子模块，用于当通过所述设备签名证书验证得到所述入域申请消息的数字签名为有效签名时，确定所述入域申请消息为有效消息。

37、根据权利要求 32 所述的证书申请装置，其特征在于，所述发送模块之后，所述证书申请装置还包括：

- 5 第一接收模块，用于接收所述车联网设备所发送的注册证书申请消息，其中所述注册证书申请消息中包含有所述入域授权令牌，且所述注册证书申请消息通过所述设备签名证书所对应的私钥进行数字签名；

获取模块，用于获取所述注册证书申请消息中的所述入域授权令牌，并获取所述入域授权令牌中的设备签名证书；

- 10 确定模块，用于当通过所述设备签名证书验证得到所述注册证书申请消息的数字签名为有效签名时，确定所述注册证书申请消息为有效消息，并向所述车联网设备发送注册证书。

38、根据权利要求 37 所述的证书申请装置，其特征在于，所述确定模块之后，所述证书申请装置还包括：

- 15 第二接收模块，用于接收所述车联网设备所发送的应用证书申请消息，其中所述应用证书申请消息中包含有所述注册证书；

基于所述应用证书申请消息，向所述车联网设备发送应用证书。

- 20 39、一种车联网设备，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，其特征在于，所述处理器执行所述计算机程序时实现如下步骤：

当车联网设备申请从第一车联网系统进入第二车联网系统时，接收所述第二车联网系统所发送的入域授权令牌；

基于所述入域授权令牌，获取所述第二车联网系统的注册证书。

- 25 40、根据权利要求 39 所述的车联网设备，其特征在于，所述接收所述第二车联网系统所发送的入域授权令牌之前，还包括：

向所述第一车联网系统发送出域申请消息；

接收所述第一车联网系统基于所述出域申请消息所发送的出域授权令牌，其中所述出域授权令牌中包含有所述车联网设备的设备签名证书；

向所述第二车联网系统发送入域申请消息，其中所述入域申请消息中包含有所述出域授权令牌，且所述入域申请消息通过所述设备签名证书所对应的私钥进行数字签名。

41、根据权利要求 40 所述的车联网设备，其特征在于，所述向所述第一车联网系统发送出域申请消息之前，还包括：

向所述第二车联网系统发送标识申请消息；

接收所述第二车联网系统基于所述标识申请消息所发送的跨域申请标识，其中所述跨域申请标识与本次进入申请相对应；

其中，所述出域申请消息和所述出域授权令牌中均包含有所述跨域申请标识。

42、根据权利要求 40 或 41 所述的车联网设备，其特征在于，所述出域授权令牌中还包含有所述车联网设备的设备信息和/或注册证书申请消息。

43、根据权利要求 40 所述的车联网设备，其特征在于，所述接收所述第二车联网系统所发送的入域授权令牌，包括：

接收所述第二车联网系统基于所述入域申请消息所发送的入域响应消息，其中，所述入域响应消息中包含有所述入域授权令牌，且所述入域授权令牌中包含有所述设备签名证书和与本次进入申请所对应的跨域申请标识。

44、根据权利要求 43 所述的车联网设备，其特征在于，所述入域授权令牌中还包含有所述车联网设备的设备信息和/或所述车联网设备在所述第二车联网系统中的设备标识；

所述入域响应消息中还包含有所述第二车联网系统中注册证书颁发机构 CA 的地址信息和/或所述第二车联网系统中应用 CA 的地址信息。

45、根据权利要求 43 所述的车联网设备，其特征在于，所述基于所述入域授权令牌，获取所述第二车联网系统的注册证书，包括：

向所述第二车联网系统发送注册证书申请消息，其中所述注册证书申请消息中包含有所述入域授权令牌，且所述注册证书申请消息通过所述设备签名证书所对应的私钥进行数字签名；

接收所述第二车联网系统基于所述注册证书申请消息所发送的注册证书。

46、根据权利要求 39 或 45 所述的车联网设备，其特征在于，所述基于所述入域授权令牌，获取所述第二车联网系统的注册证书之后，还包括：

向所述第二车联网系统发送应用证书申请消息，其中所述应用证书申请消息中包含有所述注册证书；

5 接收所述第二车联网系统基于所述应用证书申请消息所发送的应用证书。

47、一种第一车联网系统，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，其特征在于，所述处理器执行所述计算机程序时实现如下步骤：

10 当车联网设备申请从第一车联网系统进入第二车联网系统时，接收车联网设备发送的出域申请消息；

基于所述出域申请消息，向所述车联网设备发出域授权令牌，其中所述出域授权令牌中包含有所述车联网设备的设备签名证书，以使所述车联网设备向所述第二车联网系统发送入域申请消息并获取入域授权令牌，所述入域申请消息中包含有所述出域授权令牌，且所述入域申请消息通过所述设备
15 签名证书所对应的私钥进行数字签名。

48、根据权利要求 47 所述的第一车联网系统，其特征在于，所述出域申请消息和所述出域授权令牌中均包含有跨域申请标识；其中，所述跨域申请标识为所述车联网设备向所述第二车联网系统申请得到，且所述跨域申请标识与本次进入申请相对应。

20 49、根据权利要求 47 或 48 所述的第一车联网系统，其特征在于，所述出域授权令牌中还包含有所述车联网设备的设备信息和/或注册证书申请消息。

25 50、一种第二车联网系统，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，其特征在于，所述处理器执行所述计算机程序时实现如下步骤：

当车联网设备申请从第一车联网系统进入第二车联网系统时，向所述车联网设备发送入域授权令牌，以使所述车联网设备基于所述入域授权令牌获取所述第二车联网系统的注册证书。

51、根据权利要求 50 所述的第二车联网系统，其特征在于，所述向所述车联网设备发送入域授权令牌，包括：

接收所述车联网设备所发送的入域申请消息，其中所述入域申请消息中包含有出域授权令牌，所述出域授权令牌由所述车联网设备向所述第一车联网系统申请得到，且所述出域授权令牌中包含有所述车联网设备的设备签名证书，所述入域申请消息通过所述设备签名证书所对应的私钥进行数字签名；

基于所述入域申请消息，向所述车联网设备发送入域响应消息，其中，所述入域响应消息中包含有入域授权令牌，且所述入域授权令牌中包含有所述设备签名证书和与本次进入申请所对应的跨域申请标识。

52、根据权利要求 51 所述的第二车联网系统，其特征在于，所述接收所述车联网设备所发送的入域申请消息之前，还包括：

接收所述车联网设备所发送的标识申请消息；

基于所述标识申请消息，向所述车联网设备发送跨域申请标识，其中所述跨域申请标识与本次进入申请相对应；

相应地，所述出域授权令牌中还包含有所述跨域申请标识。

53、根据权利要求 51 或 52 所述的第二车联网系统，其特征在于，所述出域授权令牌中还包含有所述车联网设备的设备信息和/或注册证书申请消息。

54、根据权利要求 51 所述的第二车联网系统，其特征在于，所述入域授权令牌中还包含有所述车联网设备的设备信息和/或所述车联网设备在所述第二车联网系统中的设备标识；

所述入域响应消息中还包含有所述第二车联网系统中注册证书颁发机构 CA 的地址信息和/或所述第二车联网系统中应用 CA 的地址信息。

55、根据权利要求 51 所述的第二车联网系统，其特征在于，所述基于所述入域申请消息，向所述车联网设备发送入域响应消息之前，还包括：

获取所述入域申请消息中的出域授权令牌，并获取所述出域授权令牌中的设备签名证书；

当通过所述设备签名证书验证得到所述入域申请消息的数字签名为有效

签名时，确定所述入域申请消息为有效消息。

56、根据权利要求 51 所述的第二车联网系统，其特征在于，所述向所述车联网设备发送入域授权令牌之后，还包括：

5 接收所述车联网设备所发送的注册证书申请消息，其中所述注册证书申请消息中包含有所述入域授权令牌，且所述注册证书申请消息通过所述设备签名证书所对应的私钥进行数字签名；

获取所述注册证书申请消息中的所述入域授权令牌，并获取所述入域授权令牌中的设备签名证书；

10 当通过所述设备签名证书验证得到所述注册证书申请消息的数字签名为有效签名时，确定所述注册证书申请消息为有效消息，并向所述车联网设备发送注册证书。

57、根据权利要求 56 所述的第二车联网系统，其特征在于，所述向所述车联网设备发送注册证书之后，还包括：

15 接收所述车联网设备所发送的应用证书申请消息，其中所述应用证书申请消息中包含有所述注册证书；

基于所述应用证书申请消息，向所述车联网设备发送应用证书。

58、一种非暂态计算机可读存储介质，其上存储有计算机程序，其特征在于，该计算机程序被处理器执行时实现如权利要求 1 至 8 任一项所述的证书申请方法的步骤，或者实现如权利要求 9 至 11 任一项所述的证书申请方法的步骤，或者实现如权利要求 12 至 19 任一项所述的证书申请方法的步骤。

20

1/4

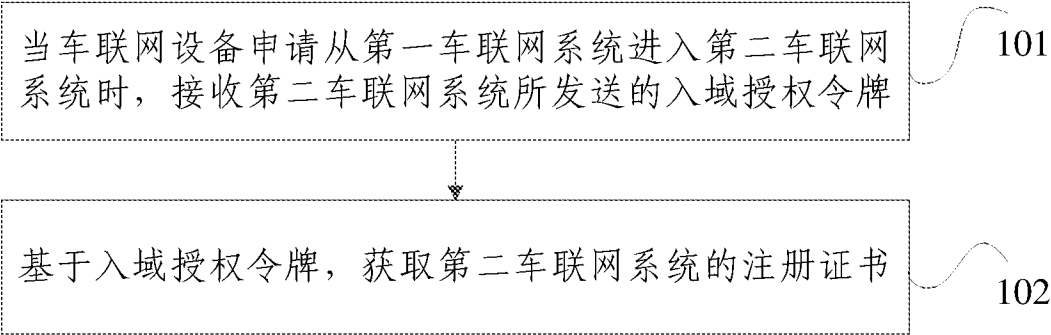


图 1

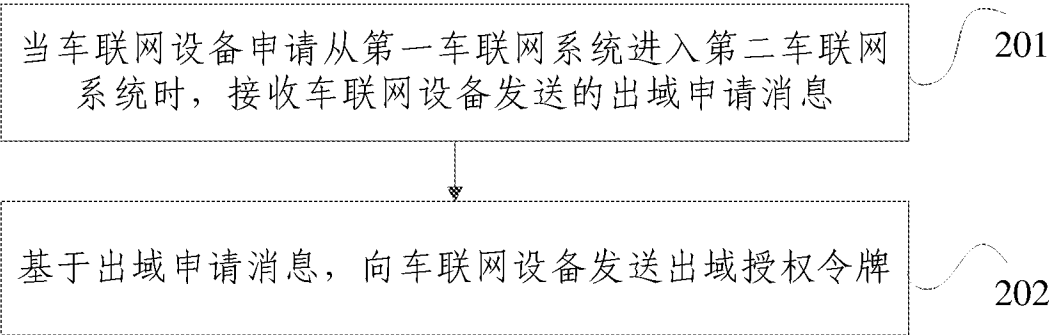


图 2



图 3

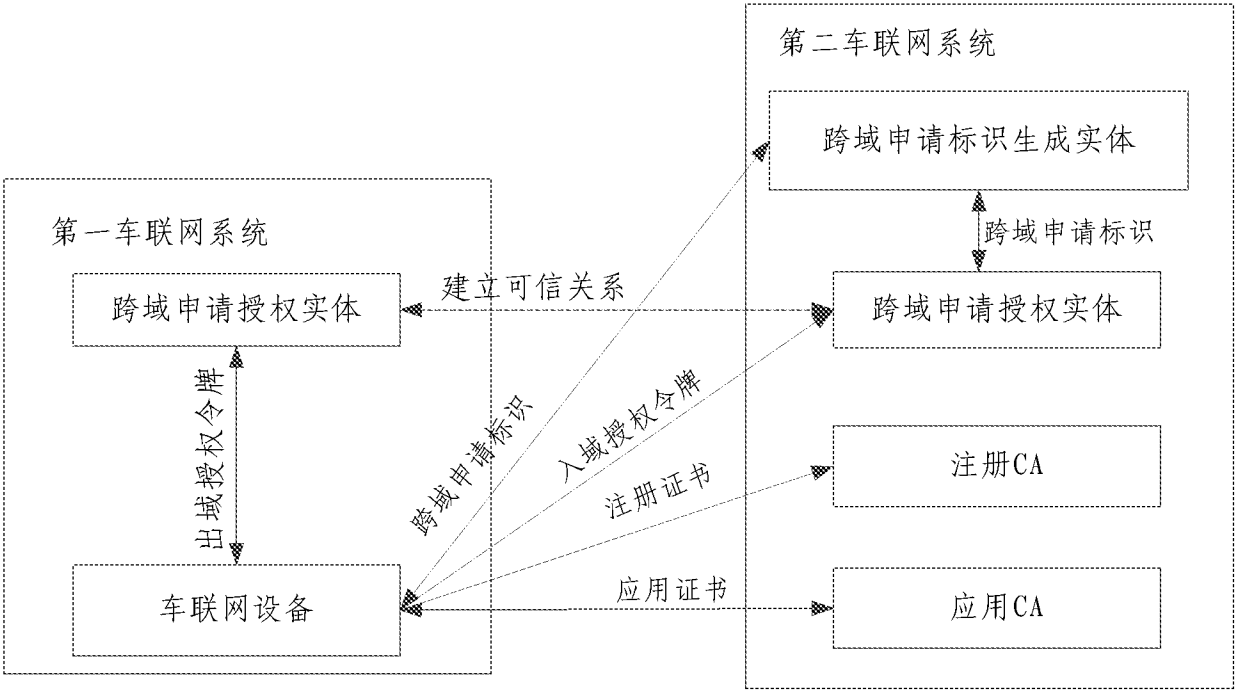


图 4

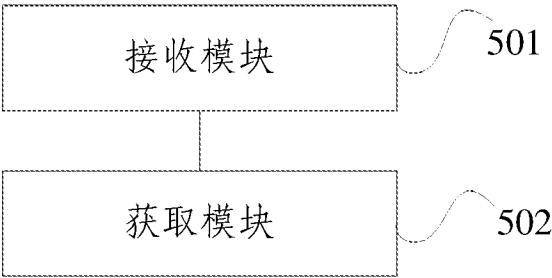


图 5

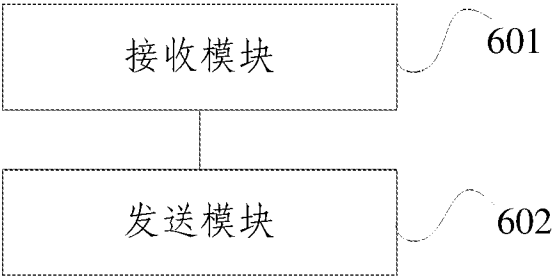


图 6

3/4



图 7

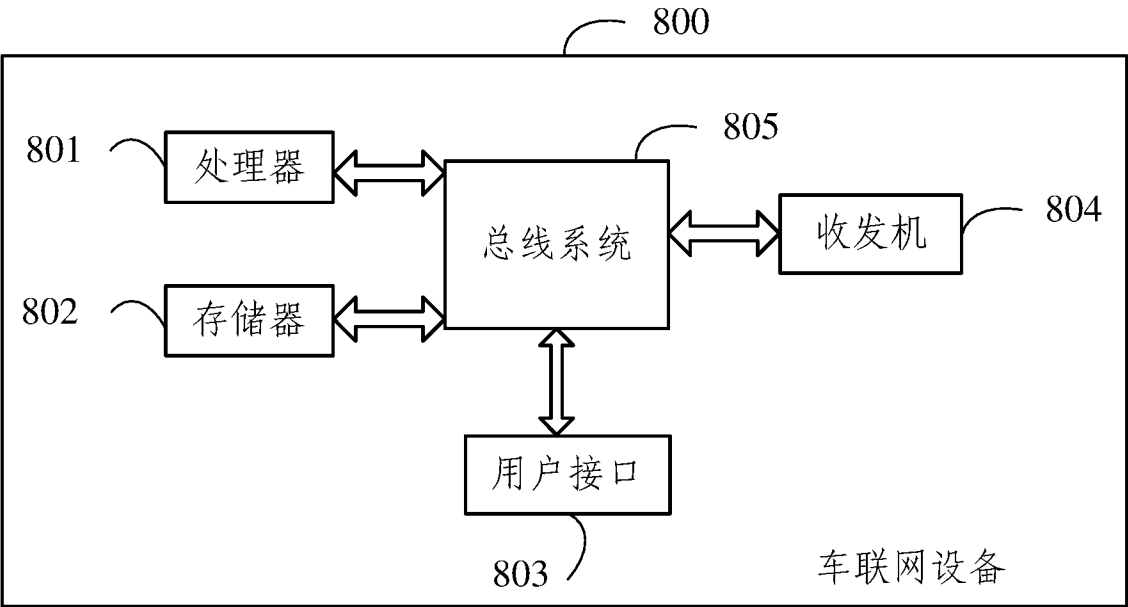


图 8

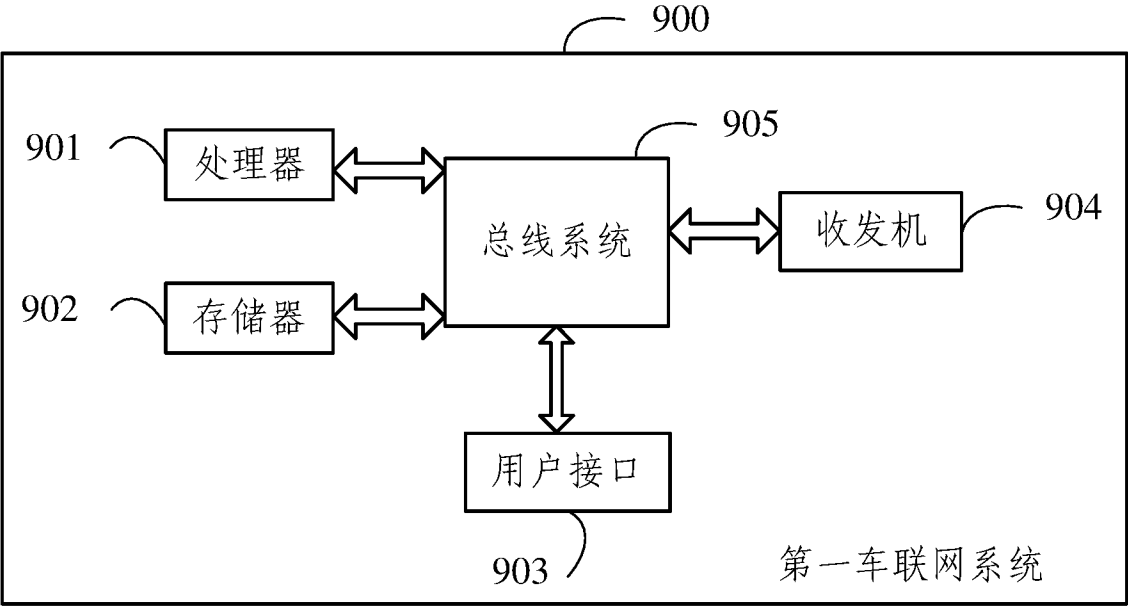


图 9

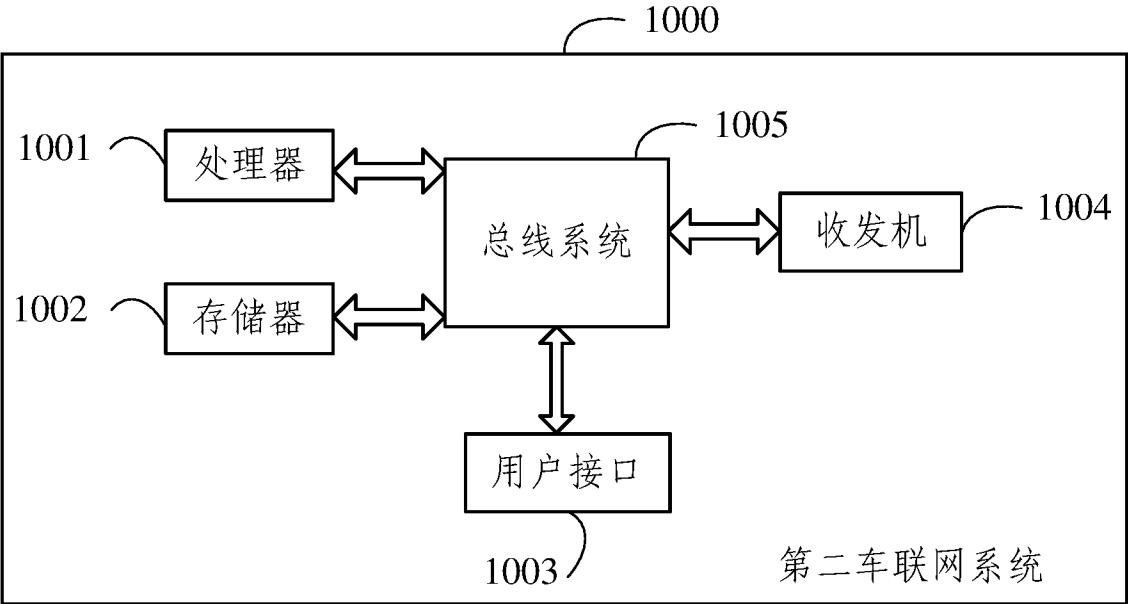


图 10

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2020/137283

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/00(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)

H04

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)

VEN, CNKI, CNABS, CNTXT, USTXT, WOTXT, EPTXT, DWPI: 签名, 车联网, 令牌, 跨系统, 第二, second, token, sign, cross

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 107359996 A (ALIBABA GROUP HOLDING LIMITED) 17 November 2017 (2017-11-17) description, pages 5-12	1-58
A	CN 1835438 A (ALIBABA CORPORATION) 20 September 2006 (2006-09-20) entire document	1-58

☐ 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

01 February 2021

Date of mailing of the international search report

18 February 2021

Name and mailing address of the ISA/CN

China National Intellectual Property Administration (ISA/
CN)No. 6, Xitucheng Road, Jimenqiao, Haidian District, Beijing
100088

China

Facsimile No. (86-10)62019451

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2020/137283

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	107359996	A	17 November 2017	CN	111783067	A	16 October 2020
				US	2019097996	A1	28 March 2019
				EP	3457627	A1	20 March 2019
				JP	2019522261	A	08 August 2019
				PH	12018502333	A1	29 July 2019
				SG	11201809238 P	A	29 November 2018
				US	2020127995	A1	23 April 2020
				TW	I659313	B	11 May 2019
				KR	20190003764	A	09 January 2019
				EP	3457627	A4	16 October 2019
				TW	201740285	A	16 November 2017
				CN	107359996	B	05 May 2020
				WO	2017193742	A1	16 November 2017
				US	10785207	B2	22 September 2020
				US	10785206	B2	22 September 2020
CN	1835438	A	20 September 2006	JP	5695120	B2	01 April 2015
				JP	2009541817	A	26 November 2009
				EP	1997271	B1	15 August 2018
				US	8589442	B2	19 November 2013
				HK	1096790	A1	08 June 2007
				WO	2007107969	A1	27 September 2007
				US	2012284190	A1	08 November 2012
				US	2007240206	A1	11 October 2007
				EP	1997271	A1	03 December 2008
				JP	2013152757	A	08 August 2013
				EP	1997271	A4	27 August 2014
				US	8250095	B2	21 August 2012
				CN	1835438	B	27 July 2011

国际检索报告

国际申请号

PCT/CN2020/137283

A. 主题的分类 H04L 9/00 (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) H04 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)) VEN, CNKI, CNABS, CNTXT, USTXT, WOTXT, EPTXT, DWPI: 签名, 车联网, 令牌, 跨系统, 第二, second, token, sign, cross											
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 107359996 A (阿里巴巴集团控股有限公司) 2017年 11月 17日 (2017 - 11 - 17) 说明书第5-12页</td> <td>1-58</td> </tr> <tr> <td>A</td> <td>CN 1835438 A (阿里巴巴公司) 2006年 9月 20日 (2006 - 09 - 20) 全文</td> <td>1-58</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 107359996 A (阿里巴巴集团控股有限公司) 2017年 11月 17日 (2017 - 11 - 17) 说明书第5-12页	1-58	A	CN 1835438 A (阿里巴巴公司) 2006年 9月 20日 (2006 - 09 - 20) 全文	1-58
类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求									
X	CN 107359996 A (阿里巴巴集团控股有限公司) 2017年 11月 17日 (2017 - 11 - 17) 说明书第5-12页	1-58									
A	CN 1835438 A (阿里巴巴公司) 2006年 9月 20日 (2006 - 09 - 20) 全文	1-58									
☐ 其余文件在C栏的续页中列出。 ☒ 见同族专利附件。											
<table border="0"> <tr> <td> * 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 </td> <td> “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 </td> </tr> </table>			* 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							
* 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 2021年 2月 1日		国际检索报告邮寄日期 2021年 2月 18日									
ISA/CN的名称和邮寄地址 中国国家知识产权局 (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		授权官员 朱少华 电话号码 86-(010)-62089391									

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2020/137283

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	107359996	A	2017年 11月 17日	CN	111783067	A	2020年 10月 16日
				US	2019097996	A1	2019年 3月 28日
				EP	3457627	A1	2019年 3月 20日
				JP	2019522261	A	2019年 8月 8日
				PH	12018502333	A1	2019年 7月 29日
				SG	11201809238P	A	2018年 11月 29日
				US	2020127995	A1	2020年 4月 23日
				TW	1659313	B	2019年 5月 11日
				KR	20190003764	A	2019年 1月 9日
				EP	3457627	A4	2019年 10月 16日
				TW	201740285	A	2017年 11月 16日
				CN	107359996	B	2020年 5月 5日
				WO	2017193742	A1	2017年 11月 16日
				US	10785207	B2	2020年 9月 22日
				US	10785206	B2	2020年 9月 22日
CN	1835438	A	2006年 9月 20日	JP	5695120	B2	2015年 4月 1日
				JP	2009541817	A	2009年 11月 26日
				EP	1997271	B1	2018年 8月 15日
				US	8589442	B2	2013年 11月 19日
				HK	1096790	A1	2007年 6月 8日
				WO	2007107969	A1	2007年 9月 27日
				US	2012284190	A1	2012年 11月 8日
				US	2007240206	A1	2007年 10月 11日
				EP	1997271	A1	2008年 12月 3日
				JP	2013152757	A	2013年 8月 8日
				EP	1997271	A4	2014年 8月 27日
				US	8250095	B2	2012年 8月 21日
				CN	1835438	B	2011年 7月 27日