(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
2023 年 9 月 28 日 (28.09.2023)

WIPO | PCT

(10) 国际公布号
WO 2023/178689 A1

(51) 国际专利分类号:
H04W 12/06 (2021.01) *H04L 9/32* (2006.01)

(21) 国际申请号: PCT/CN2022/083170

(22) 国际申请日: 2022 年 3 月 25 日 (25.03.2022)

(25) 申请语言: 中文

(26) 公布语言: 中文

(71) 申请人: **OPPO 广东移动通信有限公司 (GUANGDONG OPPO MOBILE TELECOMMUNICATIONS CORP., LTD.)** [CN/CN]; 中国广东省东莞市长安镇乌沙海滨路 18 号, Guangdong 523860 (CN)。

(72) 发明人: **甘露 (GAN, Lu)**; 中国广东省东莞市长安镇乌沙海滨路18号, Guangdong 523860 (CN)。

刘雪峰(LIU, Xuefeng); 中国广东省东莞市长安镇乌沙海滨路18号, Guangdong 523860 (CN)。 **邹继鹏(ZOU, Jipeng)**; 中国广东省东莞市长安镇乌沙海滨路18号, Guangdong 523860 (CN)。

(74) 代理人: **北京派特恩知识产权代理有限公司 (CHINA PAT INTELLECTUAL PROPERTY OFFICE)**; 中国北京市海淀区海淀南路21号中关村知识产权大厦B座2层, 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, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW,

(54) **Title:** SECURITY IMPLEMENTATION METHOD AND APPARATUS, DEVICE, AND NETWORK ELEMENT

(54) **发明名称**: 安全实现方法及装置、设备、网元

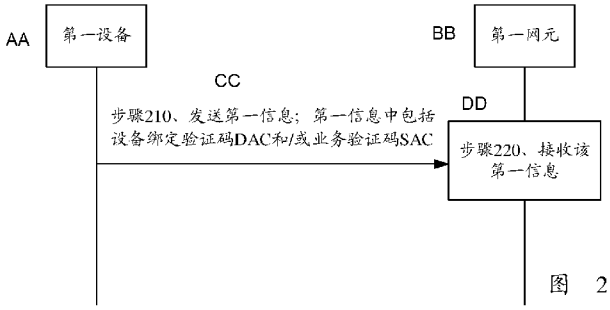

图 2

AA First device
BB First network element
CC Step 210: transmit first information, wherein the first information comprises a device authentication code (DAC) and/or a service authentication code (SAC)
DD Step 220: receive the first information

(57) **Abstract:** Embodiments of the present application provide a security implementation method and apparatus, a device, and a network element. The method comprises: a first network element receives first information, wherein the first information comprises a device authentication code (DAC) and/or a service authentication code (SAC); the DAC is used for authenticating an association relationship between a first device and at least one second device; and the SAC is used for authenticating whether the first device and/or the at least one second device support/supports a service type indicated by service identifier information, and/or whether the first device and/or the at least one second device support/supports a data type indicated by data identifier information.

(57) **摘要**: 本申请实施例提供一种安全实现方法、装置、设备及网元，该方法包括：第一网元接收第一信息；所述第一信息中包括设备绑定验证码DAC，和/或，业务验证码SAC；DAC用于验证第一设备与至少一个第二设备之间的关联关系，SAC用于验证所述第一设备和/或所述至少一个第二设备是否支持业务标识信息指示的业务类型，和/或，所述第一设备和/或所述至少一个第二设备是否支持数据标识信息指示的数据类型。

WO 2023/178689 A1

[见续页]

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, SC, 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))。

安全实现方法及装置、设备、网元

技术领域

本申请实施例涉及移动通信技术领域，具体涉及一种安全实现方法及装置、设备、网元。

背景技术

第五代移动通信技术（5th Generation Mobile Communication Technology，5G）的三大应用场景包括增强型移动宽带（eMBB）、海量机器类通信（mMTC）和超高可靠低时延通信（uRLLC）。随着通信技术的演进，工业无线传感器、视频监控和可穿戴设备等终端物联网应用对 5G 设备提出了复杂度与成本降低、尺寸减小、能耗更低等新要求。零功耗通信技术在设备的功耗、尺寸以及成本等方面将具有显著优势，从而成为了研究的热点。

然而，在零功耗设备或其他低能力设备的计算能力有限的情况下，这些设备将无法支持复杂的安全函数，因此更无法支持第三代合作伙伴计划（3rd Generation Partnership Project，3GPP）的设备认证机制。基于此，零功耗设备或其他低能力设备如何进行安全运算，以保证数据传输的安全，目前并没有明确的解决方法。

发明内容

本申请实施例提供一种安全实现方法及装置、设备、网元。

本申请实施例提供一种安全实现方法，包括：

第一网元接收第一信息；所述第一信息中包括设备绑定验证码（Device Authentication Code，DAC），和/或，业务验证码（Sercice Authentication Code，SAC）；DAC 用于验证第一设备与至少一个第二设备之间的关联关系，SAC 用于验证所述第一设备和/或所述至少一个第二设备是否支持业务标识信息指示的业务类型，和/或，所述第一设备和/或所述至少一个第二设备是否支持数据标识信息指示的数据类型。

本申请另一实施例提供一种安全实现方法，包括：

第一设备发送第一信息；所述第一设备与至少一个第二设备关联；所述第一信息中包括 DAC 和/或 SAC；所述 DAC 用于验证第一设备与至少一个第二设备之间的关联关系，所述 SAC 用于验证所述第一设备和/或所述至少一个第二设备是否支持业务标识信息指示的业务类型，和/或，所述第一设备和/或所述至少一个第二设备是否支持数据标识信息指示的数据类型。

本申请实施例提供一种安全实现装置，应用于第一网元，包括：

第一接收单元，被配置为接收第一信息；所述第一信息中包括 DAC 和/或 SAC；所述 DAC 用于验证第一设备与至少一个第二设备之间的关联关系，所述 SAC 用于验证所述第一设备和/或所述至少一个第二设备是否支持业务标识信息指示的业务类型，和/或，所述第一设备和/或所述至少一个第二设备是否支持数据标识信息指示的数据类型。

本申请实施例提供一种安全实现装置，应用于第一设备，所述第一设备与至少一个第二设备关联；包括：

第二发送单元，被配置为发送第一信息；所述第一信息中包括 DAC 和/或 SAC；DAC 用于验证第一设备与至少一个第二设备之间的关联关系，SAC 用于验证所述第一设备和/或所述至少一个第二设备是否支持业务标识信息指示的业务类型，和/或，所述第一设备和/或所述至少一个第二设备是否支持数据标识信息指示的数据类型。

本申请实施例提供的第一网元，包括处理器和存储器。该存储器用于存储计算机程序，该处理器用于调用并运行该存储器中存储的计算机程序，执行上述的安全实现方法。

本申请实施例提供的第一设备，包括处理器和存储器。该存储器用于存储计算机程序，该处理器用于调用并运行该存储器中存储的计算机程序，执行上述的安全实现方法。

本申请实施例提供的芯片，用于实现上述的安全实现方法。

具体地，该芯片包括：处理器，用于从存储器中调用并运行计算机程序，使得安装有该芯片的

设备执行上述的安全实现方法。

本申请实施例提供的计算机可读存储介质，用于存储计算机程序，该计算机程序使得计算机执行上述的安全实现方法。

本申请实施例提供的计算机程序产品，包括计算机程序指令，该计算机程序指令使得计算机执行上述的安全实现方法。

本申请实施例提供的计算机程序，当其在计算机上运行时，使得计算机执行上述的安全实现方法。

本申请实施例提供的安全实现方法，其中，第一设备可以发送第一信息；所述第一设备与至少一个第二设备关联；所述第一信息中包括设备绑定验证码 DAC，和/或，业务验证码 SAC；DAC 用于验证所述第一设备与所述至少一个第二设备之间的关联关系，SAC 用于验证所述第一设备和/或所述至少一个第二设备是否支持业务标识信息指示的业务类型，和/或，所述第一设备和/或所述至少一个第二设备是否支持数据标识信息指示的数据类型。也就是说，第二设备可以借助第一设备的运算和/或通信机制实现安全运算，提高数据传输安全。

附图说明

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

图 1 是本申请实施例提供的一种示例性的通信系统的网络架构示意图；

图 2 是本申请实施例提供的一种安全实现方法流程示意图一；

图 3 是本申请实施例提供的一种安全实现方法流程示意图二；

图 4 是本申请实施例提供的一种安全实现方法流程示意图三；

图 5 是本申请实施例提供的一种安全实现方法流程示意图四；

图 6 是本申请实施例提供的一种安全实现方法流程示意图五；

图 7 是本申请实施例提供的一种安全实现装置 700 的结构组成示意图；

图 8 是本申请实施例提供的一种安全实现装置 800 的结构组成示意图；

图 9 是本申请实施例提供的一种通信设备示意性结构图；

图 10 是本申请实施例的芯片的示意性结构图；

图 11 是本申请实施例提供的一种通信系统的示意性框图。

具体实施方式

下面将结合本申请实施例中的附图，对本申请实施例中的技术方案进行描述，显然，所描述的实施例是本申请一部分实施例，而不是全部的实施例。基于本申请中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本申请保护的范围。

图 1 是本申请实施例的一个应用场景的示意图。

如图 1 所示，通信系统 100 可以包括终端设备 110 和网络设备 120。网络设备 120 可以通过空口与终端设备 110 通信。终端设备 110 和网络设备 120 之间支持多业务传输。

应理解，本申请实施例仅以通信系统 100 进行示例性说明，但本申请实施例不限定于此。也就是说，本申请实施例的技术方案可以应用于各种通信系统，例如：长期演进（Long Term Evolution，LTE）系统、LTE 时分双工（Time Division Duplex，TDD）、通用移动通信系统（Universal Mobile Telecommunication System，UMTS）、物联网（Internet of Things，IoT）系统、窄带物联网（Narrow Band Internet of Things，NB-IoT）系统、增强的机器类型通信（enhanced Machine-Type Communications，eMTC）系统、5G 通信系统（也称为新无线（New Radio，NR）通信系统），或未来的通信系统等。

在图 1 所示的通信系统 100 中，网络设备 120 可以是与终端设备 110 通信的接入网设备。接入网设备可以为特定的地理区域提供通信覆盖，并且可以与位于该覆盖区域内的终端设备 110（例如 UE）进行通信。

网络设备 120 可以是长期演进（Long Term Evolution，LTE）系统中的演进型基站（Evolutional Node B，eNB 或 eNodeB），或者是下一代无线接入网（Next Generation Radio Access Network，NG RAN）设备，或者是 NR 系统中的基站（gNB），或者是云无线接入网络（Cloud Radio Access Network，CRAN）中的无线控制器，或者该网络设备 120 可以为中继站、接入点、车载设备、可穿戴设备、集线器、

交换机、网桥、路由器，或者未来演进的公共陆地移动网络（Public Land Mobile Network，PLMN）中的网络设备等。

终端设备 110 可以是任意终端设备，其包括但不限于与网络设备 120 或其它终端设备采用有线或者无线连接的终端设备。

例如，所述终端设备 110 可以指接入终端、用户设备（User Equipment，UE）、用户单元、用户站、移动站、移动台、远方站、远程终端、移动设备、用户终端、终端、无线通信设备、用户代理或用户装置。接入终端可以是蜂窝电话、无绳电话、会话启动协议（Session Initiation Protocol，SIP）电话、IoT 设备、卫星手持终端、无线本地环路（Wireless Local Loop，WLL）站、个人数字处理（Personal Digital Assistant，PDA）、具有无线通信功能的手持设备、计算设备或连接到无线调制解调器的其它处理设备、车载设备、可穿戴设备、5G 网络中的终端设备或者未来演进网络中的终端设备等。

终端设备 110 可以用于设备到设备（Device to Device，D2D）的通信。

无线通信系统 100 还可以包括与基站进行通信的核心网设备 130，该核心网设备 130 可以是 5G 核心网（5G Core，5GC）设备，例如，接入与移动性管理功能（Access and Mobility Management Function，AMF），又例如，认证服务器功能(Authentication Server Function，AUSF)，又例如，用户面功能（User Plane Function，UPF），又例如，会话管理功能（Session Management Function，SMF）。可选地，核心网络设备 130 也可以是 LTE 网络的分组核心演进（Evolved Packet Core，EPC）设备，例如，会话管理功能+核心网络的数据网关（Session Management Function + Core Packet Gateway，SMF+PGW-C）设备。应理解，SMF+PGW-C 可以同时实现 SMF 和 PGW-C 所能实现的功能。在网络演进过程中，上述核心网设备也有可能叫其它名字，或者通过对核心网的功能进行划分形成新的网络实体，对此本申请实施例不做限制。

通信系统 100 中的各个功能单元之间还可以通过下一代网络（next generation，NG）接口建立连接实现通信。

例如，终端设备通过 NR 接口与接入网设备建立空口连接，用于传输用户面数据和控制面信令；终端设备可以通过 NG 接口 1（简称 N1）与 AMF 建立控制面信令连接；接入网设备例如下一代无线接入基站（gNB），可以通过 NG 接口 3（简称 N3）与 UPF 建立用户面数据连接；接入网设备可以通过 NG 接口 2（简称 N2）与 AMF 建立控制面信令连接；UPF 可以通过 NG 接口 4（简称 N4）与 SMF 建立控制面信令连接；UPF 可以通过 NG 接口 6（简称 N6）与数据网络交互用户面数据；AMF 可以通过 NG 接口 11（简称 N11）与 SMF 建立控制面信令连接；SMF 可以通过 NG 接口 7（简称 N7）与 PCF 建立控制面信令连接。

图 1 示例性地示出了一个接入网设备、一个核心网设备和两个终端设备，可选地，该无线通信系统 100 可以包括多个基站设备并且每个基站的覆盖范围内可以包括其它数量的终端设备，本申请实施例对此不做限定。

需要说明的是，图 1 只是以示例的形式示意本申请所适用的系统，当然，本申请实施例所示的方法还可以适用于其它系统。此外，本文中术语“系统”和“网络”在本文中常被可互换使用。本文中术语“和/或”，仅仅是一种描述关联对象的关联关系，表示可以存在三种关系，例如，A 和/或 B，可以表示：单独存在 A，同时存在 A 和 B，单独存在 B 这三种情况。另外，本文中字符“/”，一般表示前后关联对象是一种“或”的关系。还应理解，在本申请的实施例中提到的“指示”可以是直接指示，也可以是间接指示，还可以是表示具有关联关系。举例说明，A 指示 B，可以表示 A 直接指示 B，例如 B 可以通过 A 获取；也可以表示 A 间接指示 B，例如 A 指示 C，B 可以通过 C 获取；还可以表示 A 和 B 之间具有关联关系。还应理解，在本申请的实施例中提到的“对应”可表示两者之间具有直接对应或间接对应的关系，也可以表示两者之间具有关联关系，也可以是指示与被指示、配置与被配置等关系。还应理解，在本申请的实施例中提到的“预定义”或“预定义规则”可以通过在设备(例如，包括终端设备和网络设备)中预先保存相应的代码、表格或其他可用于指示相关信息的方式来实现，本申请对于其具体的实现方式不做限定。比如预定义可以是指协议中定义的。还应理解，本申请实施例中，所述“协议”可以指通信领域的标准协议，例如可以包括 LTE 协议、NR 协议以及应用于未来的通信系统中的相关协议，本申请对此不做限定。

为便于理解本申请实施例的技术方案，以下通过具体实施例详述本申请的技术方案。以上相关技术作为可选方案与本申请实施例的技术方案可以进行任意结合，其均属于本申请实施例的保护范围。本申请实施例包括以下内容中的至少部分内容。

零功耗通信技术在设备的功耗、尺寸以及成本等方面将具有显著优势。例如，零功耗通信技术从功耗上有望将设备功耗从窄带物联网（Narrow Band Internet of Things, NB-IoT）设备的数十毫瓦的

功耗降低至几十微瓦甚至数微瓦;从成本上有望将设备成本从最便宜的NB-IoT设备的十几元降低至1元甚至更低。零功耗通信技术的主要特点是通过调制来波信号实现反向散射通信，同时它还可以通过能量采集获得能量以驱动数字逻辑电路或芯片（如微控制单元或传感器芯片），实现对信号的编码、加密或简单计算等功能。

然而，零功耗通信技术中射频能量的转化效率往往不足10%，决定了驱动数字逻辑电路或芯片用于计算的功耗要求不能太高。虽然随着工艺的改进和设计的优化有所提高，每微焦耳能量可使用于计算的次数增多，但是仍不能满足复杂的计算。零功耗终端设备计算功能非常有限，无法支持如SHA-256定义的安全函数，更无法支持3GPP的认证机制。因此，需要为零功耗设备设计轻量级的群组证书机制，以便对上行数据传输进行授权，避免攻击者或者伪基站恶意触发零功耗设备的上行数据传输，保证零功耗设备的上行传输数据的安全，提高零功耗设备授权的效率。

基于此，本申请实施例提供一种安全实现方法，参考2所示，该方法包括但不限于以下步骤:

步骤210、第一设备发送第一信息；第一信息中可以包括设备绑定验证码DAC，和/或，业务验证码SAC；其中，DAC用于验证第一设备与至少一个第二设备之间的关联关系，SAC用于验证第一设备和/或至少一个第二设备是否支持业务标识信息指示的业务类型，和/或，第一设备和/或至少一个第二设备是否支持数据标识信息指示的数据类型。

步骤220、第一网元接收该第一信息。

本申请实施例中，第一设备可以是支持设备认证机制算法的设备，例如，第一设备可以是UE，基站，或者其他可支持复杂运算的设备，本申请实施例对此不做限制。

第二设备可以是不支持设备认证机制算法的低运算能力的设备，即第二设备是无法单独进行安全运算的设备，例如，第二设备可以是零功耗设备（Zero Power Device，ZPD），或者运算能力较弱的低能力设备，或者剩余电量较少的设备，本申请实施例对此不做限制。

第一网元可以是位于网络中的设备。示例性的，第一网元可以是至少一个第二设备的厂商提供的应用服务器或设备ID管理服务器，也可以是运营商提供的接入网设备(例如基站)或核心网设备，也可以是业务提供商（SP）提供的服务器或设备ID管理服务器。本申请实施例对此不做限制。

可选地，第二设备可以与第一设备通过调制来波信号实现反向散射的技术进行通信。

本申请实施例中，第一设备可以与一个或者多个第二设备进行关联。应理解，第一设备是支持设备认证机制的设备，与第一设备关联的至少一个第二设备可以利用该第一设备的运算和/或通信机制，实现安全运算。

具体地，本申请实施例中，第一设备可以向第一网元发送第一信息，通过第一信息携带DAC和/或SAC。这样，第一网元可以基于第一信息中的DAC和/或SAC，对与第一设备关联的至少一个第二设备进行验证，以便于与至少一个第二设备进行数据交互，或者第一网元可以基于DAC和/或SAC，为至少一个第二设备生成授权凭证，以保证第二设备数据传输的安全。

需要说明的是，第一信息可以是第一设备直接发送给第一网元，也可以是第一设备通过其他中间设备转发给第一网元，本申请实施例对此不做限制。示例性的，当第一网元为接入网设备或和核心网设备时，第一设备可以直接向该第一网元发送第一信息。当第一网元为应用服务器或设备ID管理服务器时，第一设备可以通过运营商提供的接入网设备和/或核心网设备，向该第一网元转发上述第一信息。

可选地，第一网元接收到第一信息后，可以基于DAC验证第一设备与至少一个第二设备之间是否真实存在关联关系，从而确定是否可以信任至少一个第二设备。

可选地，第一网元可以基于SAC，验证第一设备和/或第二设备支持的业务类型是否是业务标识信息指示的业务类型，从而确定第一设备和/至少一个第二设备是否具有传输该业务类型对应的数据的权限。

可选地，第一网元还可以基于SAC，验证第一设备和/或第二设备支持的数据类型是否是数据标识信息指示的数据类型，从而确定第一设备和/至少一个第二设备是否具有传输该数据类型对应的数据的权限。

本申请实施例中，第一设备和/或至少一个第二设备可以提供一种或多种业务，例如定位业务、测速业务、健康呼救业务、环境监测业务等。本申请实施例可以通过业务标识信息来指示第一设备和/或至少一个第二设备提供的业务类型。

可选地，业务标识信息可以是业务类型的ID，也可以是第一设备和/或至少一个第二设备的厂商提供的应用服务器的ID，或者业务提供商提供的应用服务器的ID。示例性的，当第一网元为业务提供商（SP）提供的应用服务器时，第一网元的ID与业务标识信息相同。

本申请实施例中，数据标识信息可以指示第一设备和/或至少一个第二设备支持的数据类型，该数据类型包括一种或多种。通常情况下，设备所支持的数据类型通常与设备所支持的业务相关。示例性的，如果该业务为健康呼救业务，那么数据类型可以包括心率数据、体温数据、呼吸频率数据、运动量数据、血压数据等，如果感知业务为环境监测业务，那么数据类型可以包括位置数据、风速数据、温度数据、日晒数据、高度数据等。本申请实施例对数据类型不做限制。

可选地，上述业务标识信息和数据标识信息可以通过第一信息携带。业务标识信息和数据标识信息也可以是第一网元预存储的，本申请实施例对此不做限制。

由此可见，本申请实施例提供的安全实现方法中，第一设备可以做为第二设备的中间代理，通过第一设备完备的运算和/或通信机制为第二设备实现安全运算，提高数据传输安全。

可选地，第一信息可以是凭证请求信息，也就是说，该第一信息可以用于请求与第一设备关联的至少一个第二设备的授权凭证。

可以理解的是，第一设备可以利用其自身的运算和/或通信机制，向网络侧的网元请求与其关联的至少一个第二设备的授权凭证。

对应的，参考图 3 所示，本申请实施例提供的安全实现方法中还可以包括以下步骤：

步骤 230、在第一网元对 DAC 和/或 SAC 验证通过的情况下，第一网元为至少一个第二设备生成授权凭证。

本申请实施例中，第一网元接收到第一信息之后，可以通过 DAC 来确定第一设备与至少一个第二设备之间具有真实的关联关系，通过 SAC 来验证第一设备和/或至少一个第二设备支持的业务类型是否是业务标识信息指示的业务类型，和/或，第一设备和/或至少一个第二设备支持的数据类型是否是数据标识信息指示的数据类型。

应理解，只有在第一网元确定了第一设备和至少一个第二设备之间的关联关系是正确的，且第一设备和/或至少一个第二设备支持的业务类型为业务标识信息所指示的业务类型，和/或，第一设备和/或至少一个第二设备支持的数据类型为数据标识信息所指示的数据类型的情况下，第一网元才为至少一个第二设备生成授权凭证。

可选地，若第一信息是第一设备通过接入网设备和/或核心网设备转发给第一网元的，那么第一信息的转发设备（也就是接入网设备和/或核心网设备）可以对第一信息中的 DAC 进行验证，并且，该转发设备可以在对 DAC 验证通过之后，根据业务标识信息，将该第一信息发送给第一网元。进而，第一网元可以继续对 SAC 进行验证，并在对 SAC 验证通过后，生成至少一个第二设备的授权凭证。

综上所述，本申请实施例提供的安全实现方法中，第一设备可以作为中间代理设备，为第一设备关联的至少一个第二设备实现安全运算，以获得至少一个第二设备的授权凭证。也就是说，可以借用第一设备与第一网元进行交互，以使第一网元为至少一个第二设备生成轻量级的授权凭证，使设备获得业务授权，提高业务安全和数据传输安全。

可选地，参考图 3 所示，本申请实施例提供的安全实现方法中，步骤 210 之前，还可以包括以下内容：

步骤 240、第一设备基于设备秘钥 Secret，生成设备绑定验证码 DAC;

和/或，

第一设备基于第一设备的标识信息、每个第二设备的标识信息、业务标识信息、数据标识信息、随机数 NONCE、以及计数器参数 COUNT 在内的至少一项，生成业务验证码 SAC。

可选地，第一设备可以基于以下公式（1）来计算设备绑定验证码 DAC。

$$DAC=H(Secret, ID_{UE}, ID_{ZP}, S) \quad (1);$$

其中，H( )为哈希函数或校验功能或密钥生成功能函数，例如 H( )可以以为 HMAC-SHA-256、也可以为安全函数 f1、安全函数 f2、安全函数 f3、安全函数 f4、或者安全函数或 f5，本申请实施例对此不做限制。

ID_{UE} 为第一设备的标识信息，ID_{ZP} 为至少一个第二设备的标识信息。应理解，当第二设备的数量包括多个时，ID_{ZP} 可以包括多个第二设备中每个第二设备的标识信息。S 可以包括以下中的至少一项：第一设备的证书信息 $Cert_{UE}$，随机数 NONCE，以及计数器参数 COUNT。

可选的，S 还可以包括以下信息中的一个或多个：ID_{SP}，ID_{DATA}。其中，ID_{SP} 是指业务标识信息，ID_{DATA} 是指数据标识信息。

可选地，设备秘钥 Secret 可以是基于业务共享秘钥 Kservice，和/或，每个第二设备的初始秘钥生成。这里，业务共享秘钥 Kservice 是第一网元与第一设备进行安全协商后得到的对称秘钥。其中，业务共享秘钥 Kservice，可以为 K_{eNB}，K_{RRCint}，K_{RRCenc}，K_{NASenc}，K_{NASint}，K_{AF}，或 K_{s_NAF} 中的任意一个，

本申请实施例对此不做限制。

需要说明的是，步骤240中设备秘钥Secret的生成方式详见下文实施例的描述，此处不再赘述。

可选地，在一些实施例中，第一设备可以利用第一设备的私钥，对第一设备的标识信息、至少一个第二设备的标识信息、业务标识信息、数据标识信息、NONCE、以及COUNT中的至少一项信息进行签名，得到业务验证码SAC。

示例性的，第一设备可以利用以下公式（2）来生成业务验证码SAC:

$$SAC=Sig_{UE}（S）\quad（2）;$$

其中，Sig_{UE}是指使用UE的私钥进行签名的过程。S为输入参数，至少包含以下一个或多个:ID_{ZP}，ID_{UE}，ID_{SP}，ID_{DATA}，NONCE，以及COUNT。这里的ID_{SP}、ID_{DATA}、ID_{ZP}和ID_{UE}如上所述，此处不做赘述。

可选地，在另一些实施例中，第一设备可以基于业务共享秘钥Kservice，对第一设备的标识信息、每个第二设备的标识信息、业务标识信息、数据标识信息、NONCE、以及COUNT中的至少一项进行安全运算，生成SAC。

示例性的，第一设备可以利用以下公式（3）来生成业务验证码SAC:

$$SAC=H（Kservice，S）\quad（3）;$$

其中，S为输入参数，可以包括以下信息中的一个或多个:ID_{ZP}，ID_{UE}，ID_{SP}，ID_{DATA}，NONCE，COUNT。其中，ID_{ZP}，ID_{UE}，ID_{SP}，和ID_{DATA}如上所述，此处不做赘述。

进一步地，第一设备将运算得到的DAC和/或SAC通过第一信息发送给第一网元，以使第一网元为第一设备关联的至少一个第二设备生成授权凭证。

本申请实施例中，第一网元在接收到第一信息后，可以对DAC和/或SAC进行验证。以下详细介绍第一网元对DAC和SAC的验证过程。

本申请实施例中，第一网元接收到第一信息后，可以通过DAC来验证第一设备与至少一个第二设备之间是否具有真实的关联关系，通过SAC来验证第一设备和/或至少一个第二设备支持的业务类型是否是业务标识信息指示的业务类型，和/或，第一设备和/或至少一个第二设备支持的数据类型是否是数据标识信息指示的数据类型。

其中，第一网元对DAC的验证过程如下:

第一网元可以基于设备秘钥Secret，生成第一校验信息。其中，第一网元可以参考上述公式（1）来生成第一校验信息。若第一校验信息与第一信息中携带的DAC一致，可以认为第一设备和至少一个第二设备之间真实存在关联关系，第一设备确定DAC验证通过。若第一校验信息与第一信息中携带的DAC不一致，则认为第一设备与至少一个第二设备之间的关联关系错误或不存在，第一网元确定DAC验证不通过。

可选地，第一网元可以从第一设备处获取设备秘钥Secret，也可以从其他受信任的设备（例如基站、UDM网元、应用服务器等）处获取设备秘钥Secret。第一网元还可以基于业务共享秘钥，和/或，每个第二设备的初始秘钥生成该设备秘钥Secret，其中，第一网元生成设备秘钥Secret的方式与第一设备生成设备秘钥Secret的方式相同。本申请实施例确定设备秘钥Secret的方式不做限制。

另外，第一网元对SAC的验证过程如下:

可选地，在一些实施例中，若SAC是利用第一设备的私钥对第一设备的标识信息、每个第二设备的标识信息、业务标识信息、以及数据标识信息、NONCE、以及COUNT在内的至少一项信息进行签名得到，则第一网元可以利用第一设备的公钥对SAC进行验证。

具体地，第一网元可以通过第一设备的公钥对SAC进行验证，得到第二校验信息。若第二校验信息与第一信息中包括的第一设备的标识信息、至少一个第二设备的标识信息、业务标识信息、数据类型标识信息、NONCE、以及COUNT在内的至少一项信息一致，则认为第一设备和/或至少一个第二设备支持的业务类型与业务标识信息指示的业务类型相同，以及第一设备和/或至少一个第二设备支持的数据类型为数据标识信息所指示的数据类型，第一网元确定SAC验证通过。否则，确定SAC验证不通过。

可选地，在另一些实施例中，若SAC是利用业务共享秘钥Kservice，对第一设备的标识信息、每个第二设备的标识信息、业务标识信息、数据标识信息、NONCE、以及COUNT中的至少一项进行安全运算得到，则第一网元可以利用业务共享秘钥Kservice，对SAC进行验证

具体地，第一网元首先可以基于业务共享秘钥Kservice，对第一设备的标识信息、每个第二设备的标识信息、业务标识信息、数据标识信息、NONCE、以及COUNT中的至少一项进行安全运算，得到第三校验信息；其中，第一网元可以参考上述公式（3）来生成第三校验信息。若第三校验信息

与所述 SAC 一致，则第一网元确定 SAC 验证通过。否者，确定 SAC 验证不通过。

可选地，若第一信息是第一设备通过接入网设备和/或核心网设备转发给第一网元的，那么第一信息的转发设备（也就是接入网设备和/或核心网设备）也可以对第一信息中的 DAC 进行验证，并且，该转发设备可以在对 DAC 验证通过之后，根据业务标识信息，将该第一信息发送给第一网元。进而，第一网元可以继续对 SAC 进行验证，并在对 SAC 验证通过后，生成至少一个第二设备的授权凭证。

需要说明的是，接入网设备和/或核心网设备对DAC进行验证的方式与上文中描述的方式相同，为了简洁，此处不再赘述。

另外，若第一网元为接入网设备和/或核心网设备，则可以直接对第一信息中携带的 DAC 和/或 SAC 进行验证。

可选地，考虑到 DAC 和/或 SAC 的验证过程需要进行复杂的安全运算，因此，本申请实施例中，在 DAC 和/或 SAC 进行验证之前，还可以根据第一信息中的内容进行一些初步的验证，避免进行不必要的 DAC 和/或 SAC 验证。

示例性的，第一网元可以维护一份设备列表，该设备列表中存储第一网元支持的所有设备的标识信息。当第一信息中包括第一设备的标识信息和/或至少一个第二设备的标识信息时，第一网元可以判断设备列表中是否包括第一信息中的第一设备的标识信息和/或至少一个第二设备的标识信息。若第一设备的标识信息和至少一个第二设备的标识信息不在设备列表中，则可以确定第一网元不支持与第一设备和/或第二设备进行数据传输，那么第一网元可以不进行进一步操作，即不进行复杂的 DAC 和/或 SAC 验证。否则，第一网元需要继续进行 DAC 和/或 SAC 验证。

第一网元还可以维护一份业务类型列表，该业务类型列表用于存储第一网元支持的业务类型。当第一信息中包括业务标识信息时，第一网元可以从业务类型列表中查找是否包括该业务标识信息对应的业务类型。若该业务类型列表中不包括该业务类型，则说明第一网元不支持该业务类型，这样，第一网元可以避免进行 DAC 和/或 SAC 验证。

另外，第一网元还可以维护一份数据类型列表、该数据类型列表用于存储第一网元支持的数据类型。当第一信息中包括数据标识信息时，第一网元可以从数据类型列表中查找是否包括该数据标识信息对应的数据类型。若该数据类型列表中不包括该数据类型，则说明第一网元不支持该数据类型，这样，第一网元可以避免进行 DAC 和/或 SAC 验证。

可选地，上述设备列表、业务类型列表、以及数据类型列表中的信息可以是第一网元通过调用其他数据库设备存储的信息获取得到。

综上所述，第一网元可以根据 DAC 和/或 SAC 确定第一设备和至少一个第二设备具有绑定关系，以及第一设备和/或第二设备与业务标识信息指示的业务类型绑定，第一设备和/或第二设备与数据标识信息指示的数据类型绑定；只有在上述至少一项绑定关系成立的前提下，第一网元才可以为至少一个第二设备生成授权凭证，如此保证生成的授权凭证的安全性。

可选地，第一信息除了包括 DAC 和/或 SAC 之外，还包括以下中的至少一项：

业务标识信息；

数据标识信息；

第一设备的标识信息；

至少一个第二设备中每个第二设备的标识信息；

设备秘钥 Secret；

第一信息对应的第一信息验证码 MAC；第一 MAC 用于验证所述第一信息的发送方是否为合法设备。

可选地，第一网元在对 DAC 和/SAC 进行验证之前，还可以先对发送第一信息的第一设备进行身份验证。只有在对第一设备的身份验证通过之后，才进一步地对 DAC 和/SAC 进行验证。否则，第一设备的身份验证未通过，第一网元可以认为发送第一信息的设备为不可信任的设备，不对第一信息进行响应。

可选地，在第一信息中包括第一 MAC 的情况下，第一网元可以根据该第一 MAC 对第一设备进行身份验证。

在一种可能的实现方式中，若第一 MAC 是第一设备基于其与第一网元之间的业务共享秘钥生 Kservice 成的，则第一网元可以使用该业务共享秘钥 Kservice 生成校验信息，若校验信息与第一 MAC 一致，则确定第一设备的身份验证通过。

可选地，第一设备与第一网元预先协商好的业务共享秘钥 Kservice 可以是秘钥 K_{eNB}，K_{RRCint}，

K_{RRCenc}, K_{NASenc}, K_{NASint}, K_{AF}, K_{s_NAF} 等，本申请实施例对此不做限制。

在另一种可能的实现方式中，若第一 MAC 是第一设备利用其私钥对第一信息中的其他信息签名得到，则第一网元可以使用第一设备的公钥对第一 MAC 验证，若验证结果与第一信息中的其他信息一致，则确定第一设备的身份验证通过。在对第一设备的身份验证通过的情况下，第一网元进一步对 DAC 和/或 SAC 进行验证，确定是否为至少一个第二设备生成授权凭证。

本申请实施例中，第一网元在对 DAC 和/或 SAC 验证通过后，可以为至少一个第二设备生成授权凭证。其中，至少一个第二设备可以共用一个授权凭证。

可选地，在第一网元生成授权凭证之前，可以为每个第二设备生成 RSA 累加器参数 α_{ZP}，每个第二设备的 RSA 累加器参数 α_{ZP} 可以用于证明该第二设备的是否被撤销。

可选地，第一网元生成的授权凭证中可以包括以下信息中的至少一项：

第一设备的标识信息；

第一设备的公钥；

至少一个第二设备中每个第二设备的标识信息；

至少一个第二设备中每个第二设备的 RSA 累加器参数；

第一网元的标识信息；

第一网元的公钥；

业务标识信息；

数据标识信息；

设备绑定验证码 DAC；

第一网元的数字签名。

其中，数字签名可以是第一网元利用自己的私钥对上述授权凭证中的其他信息进行签名得到。应理解，该数字签名可以用于验证该授权凭证的合法性。

在一示例中，第二设备的数量为 1 时，该第二设备 ZP1 的授权凭证可以为：$Cert_{IS->ZP}$（[ID_{ZP1}，DAC]，α_{ZP1}，ID_{UE}，ID_{IS}，ID_{SP}，Sig_{skIS}）。其中，IS 是指第一网元，$Cert_{IS->ZP}$ 可以理解为是第一网元为第二设备生成的授权凭证。α_{ZP1} 为第二设备 ZP1 的 RSA 累加器参数，ID_{IS} 为第一网元的标识信息，sk_{IS} 为第一网元的私钥，Sig_{skIS} 为第一网元的数字签名。

在另一示例中，第二设备的数量为 n 时，n 为大于 1 的整数，该 n 个第二设备的授权凭证可以为：$Cert_{IS->ZPg}$（[ID_{ZP1}，…，ID_{ZPn}，DAC]，α_{ZP1}，…，α_{ZPn}，ID_{UE}，ID_{IS}，ID_{SP}，Sig_{skIS}）。其中，α_{ZP1}，…，α_{ZPn} 分别为 n 个第二设备对应的 RSA 累加器参数。

需要说明的是，当业务标识信息 ID_{SP} 为应用服务器的 ID，且第一网元为该应用服务器时，第一网元的标识信息 ID_{IS} 与业务标识信息 ID_{SP} 相同，第一网元可以仅使用其中的一种来生成授权凭证。

应理解，第二设备的数量包括多个时，第一网元可以为多个第二设备生成一个授权凭证，该授权凭证可以是群组证书，即多个第二设备可以共用一个授权凭证。

可选地，参考图 4 所示的流程示意图，本申请实施例中，第一网元在生成至少一个第二设备的授权凭证之后，还可以执行步骤 250 和步骤 260。

步骤 250、第一网元向区块链节点发送授权凭证；

步骤 260、第一网元获取该授权凭证的存储位置信息。

可以理解的是，第一网元可以向区块链节点发送所生成的至少一个第二设备的授权凭证，对至少一个第二设备的授权凭证进行上链操作，以实现对该授权凭证的分布式存储。进一步地，区块链节点接收到授权凭证后，可以将该授权凭证存储于区块链的存储区块中，并将存储位置信息反馈给第一网元。

可选地，参考图 4 所示，步骤 260 之后还可以包括以下步骤：

步骤 270、第一网元向第一设备发送授权凭证，和/或，存储位置信息。

可以理解的是，第一网元在生成授权凭证之后，可以将生成的授权凭证发送给凭证的请求方，即第一设备。第一网元也可以将授权凭证在存储区块中的存储位置信息发送给第一设备，第一设备和/或至少一个第二设备可以在需要时根据该存储位置信息向区块链节点请求授权凭证。

以下详细介绍步骤 240 中设备秘钥 Secret 的生成方式。

本申请实施例中，步骤 240 中的设备秘钥 Secret 可以是第一设备基于业务共享秘钥 Kservice，和/或，每个第二设备对应的初始秘钥计算得到。

可选地，参考图 5 所示，步骤 240 之前还可以包括以下内容：

步骤 510、第一设备基于业务共享秘钥 Kservice，和/或，至少一个第二设备中每个第二设备的

初始秘钥，生成设备秘钥 Secret。

可选地，第一设备可以直接基于每个第二设备对应的初始秘钥，生成设备秘钥 Secret。

示例性的，若第二设备的数量为 1，则设备秘钥 Secret 即为该第二设备的初始秘钥。若第二设备的数量包括多个，则第一设备可以将每个第二设备的初始秘钥进行汇聚处理，得到上述设备秘钥 Secret。其中，汇聚处理可以是将多个秘钥直连处理。

可选地，第一设备也可以基于至少一个第二设备中每个第二设备的初始秘钥，以及业务共享秘钥 Kservice，生成设备秘钥 Secret。其中，业务共享秘钥 Kservice 可以为 K_{eNB}，K_{RRCint}，K_{RRCenc}，K_{NASenc}，K_{NASint}，K_{AF}，K_{s_NAF} 等，本申请实施例对此不做限制。

示例性的，若第二设备的数量为 1，则第一设备可以将该第二设备的初始秘钥和业务共享秘钥 Kservice 进行直连处理，得到设备秘钥 Secret。若第二设备的数量包括多个，则第一设备可以将每个第二设备的初始秘钥，以及业务共享秘钥 Kservice 进行直连处理，得到设备秘钥 Secret。

可选地，步骤 510 中第一设备基于业务共享秘钥 Kservice，和/或，至少一个第二设备中每个第二设备的初始秘钥，生成设备秘钥 Secret，还可以通过以下方式实现：

第一设备基于每个第二设备的初始秘钥，生成每个第二设备的中间秘钥；

第一设备基于业务共享秘钥 Kservice，和/或，每个第二设备的中间秘钥，生成设备秘钥 Secret。

其中，中间秘钥可以是第一设备与第二设备进行物理层安全协商后得到的可以在两个设备之间共享使用的对称秘钥。

可选地，第一设备可以先基于每个第二设备的初始秘钥，生成每个第二设备的中间秘钥；接着，第一设备可以基于至少一个第二设备中每个第二设备的中间秘钥，生成设备秘钥 Secret。

也就是说，第一设备可以基于每个第二设备的初始秘钥，与该第二设备进行物理层安全机制的协商处理，生成各个第二设备分别对应的中间秘钥。进而，第一设备可以基于每个第二设备的中间秘钥，生成设备秘钥 Secret。

示例性的，若第二设备的数量为 1，则设备秘钥 Secret 即为该第二设备的中间秘钥。若第二设备的数量包括多个，则第一设备可以将每个第二设备的中间秘钥进行汇聚处理，得到上述设备秘钥 Secret。其中，汇聚处理可以是将多个秘钥直连处理。

可选地，第一设备还可以先基于每个第二设备的初始秘钥生成每个第二设备的中间秘钥；接着，第一设备可以基于业务共享秘钥 Kservice，以及每个第二设备的中间秘钥，生成设备秘钥 Secret。

示例性的，若第二设备的数量为 1，则设备秘钥 Secret 即为该第二设备的中间秘钥。若第二设备的数量包括多个，则第一设备可以将业务共享秘钥 Kservice，和每个第二设备的中间秘钥进行汇聚处理，得到上述设备秘钥 Secret。

需要说明的是，第一网元在验证 DAC 之前，也可以通过上述方式确定设备秘钥 Secret。也就是说，第一网元可以基于业务共享秘钥 Kservice，和/或，每个第二设备的初始秘钥，生成设备秘钥 Secret。或者，第一网元可以基于每个第二设备的初始秘钥，计算每个第二设备的中间秘钥；进一步，第一网元基于业务共享秘钥 Kservice，和/或，每个第二设备的中间秘钥，生成设备秘钥 Secret。计算方式与步骤 510 中描述的方式相同，为了简洁，此处不再赘述。

可选地，参考图 5 所示，步骤 510 之前，还可以执行以下步骤：

步骤 520、第一设备向第二网元发送秘钥请求信息；该秘钥请求信息用于请求与第一设备关联的至少一个第二设备的初始秘钥。

步骤 530、第二网元向第一设备发送初始秘钥信息，该初始秘钥信息中包括所述至少一个第二设备中每个第二设备的初始秘钥。

其中，第二网元可以是上述至少一个第二设备所信任的设备，用于管理上述至少一个第二设备中每个第二设备的初始秘钥。例如，第二网元可以是上述第二设备的厂商提供的服务器或设备 ID 管理服务器，也可以是运营商提供的接入网设备或核心网设备，也可以是业务提供商（SP）提供的服务器或设备 ID 管理服务器，本申请实施例对此不做限制。

需要说明的是，第二网元与上述实施例中的第一网元可以为同一设备，也可以为不同的设备，本申请实施例对此不做限制。

可选地，秘钥请求信息中可以包括以下信息中的至少一项：

第一设备的标识信息；

至少一个第二设备中每个第二设备的标识信息；

业务标识信息；

数据标识信息；

秘钥请求信息对应的第二 MAC。

本申请实施例中，第二网元在接收到秘钥请求信息后，可以向第一设备反馈初始秘钥信息，该初始秘钥信息中可以携带至少一个第二设备的初始秘钥。具体地，初始秘钥信息中可以包括至少一个第二设备的标识信息，以及每个第二设备对应的初始秘钥。

示例性的，若第二设备的数量仅为一个，则初始秘钥信息中可以包括一个标识信息-初始秘钥对，即(ID_{ZP1}，K_{ZP1})。若第二设备的数量为多个（例如 n 个），则初始秘钥信息中可以包括 n 个标识信息-初始秘钥对：(ID_{ZP1}，K_{ZP1})，(ID_{ZP2}，K_{ZP2})，(ID_{ZP3}, K_{ZP3})，……，(ID_{ZPn}，K_{ZPn})。其中，ID_{ZP1} 即零功耗设备 1 的标识信息，K_{ZP1} 即零功耗设备 1 的初始秘钥，以此类推，ID_{ZPn} 即零功耗设备 n 的标识信息，K_{ZPn} 即零功耗设备 n 的初始秘钥。

可选地，初始秘钥可以是对称秘钥，第二设备的本地存储空间中也可以存储自己的初始秘钥。

可选地，当秘钥请求信息中包括业务标识信息和/或数据标识信息时，第二网元可以基于业务标识信息和/或数据标识信息对至少一个第二设备进行验证，判断至少一个第二设备是否具有使用该业务标识信息和/或数据标识信息对应的业务的权限。并且，只有在至少一个第二设备验证通过后，第二网元才向第一设备发送初始秘钥信息。

其中，第二网元可以判断本地存储的业务标识信息与秘钥请求信息中携带的业务标识信息是否一致，和/或，本地存储的数据标识信息与秘钥请求信息中数据标识信息是否一致。若一致，则第二网元确定至少一个第二设备验证通过，也就是说，至少一个第二设备具有使用该业务标识信息对应业务类型，和/或数据标识信息对应的数据类型的权限。若不一致，则第二网元确定至少一个第二设备验证失败，至少一个第二设备均不具有使用该业务标识信息对应业务类型，和/或数据标识信息对应的数据类型的权限。

示例性的，在第二网元为应用服务器，业务标识信息为应用服务器的 ID 的情况下，第二网元可以对比自己的 ID 与秘钥请求信息中携带的业务标识信息。若两者相同，则确定至少一个第二设备验证通过，否则，确定至少一个第二设备验证失败。

本申请实施例中，秘钥请求信息中可以包括第二 MAC。第二网元在接收到第一设备发送的秘钥请求信息后，可以先根据该第二 MAC 对第一设备的身份进行认证，以确定发送秘钥请求信息的第一设备是否是可信任的设备。

可选地，在一些实施例中，第一设备可以使用与第二网元预先协商好的秘钥来对秘钥请求信息进行加密或完成性保护，得到第二 MAC。示例性的，第一设备与第二网元预先协商好的秘钥可以是秘钥 K_{eNB}，K_{RRCint}, K_{RRCenc}, K_{NASenc}, K_{NASint}, K_{AF}，K_{s_NAF} 等，本申请实施例对此不做限制。

对应的，第二网元在接收到秘钥请求信息之后，可以利用上述与第一设备协商好的秘钥对第二 MAC 进行验证。示例性的，若第二网元为基站，则第二网元可以使用 K_{eNB} 或 K_{RRCint} 对第二 MAC 进行验证。若第二网元为应用服务器，则第二网元可以使用 K_{AF} 或 K_{s_NAF} 对第二 MAC 进行验证。若第二网元为核心网网元，则第二网元可以使用 K_{NASint}，对第二 MAC 进行验证。

可选地，在另一些实施例中，第一设备可以使用第一设备的私钥对秘钥请求信息的内容或部分内容进行签名，得到第二 MAC。对应的，第二网元在接收到秘钥请求信息后，可以利用使用第一设备的证书或者第一设备的公钥对第二 MAC 进行验证。

应理解，第二网元在对第一设备的身份认证通过后，才向第一设备发送初始秘钥信息。

下面结合具体应用场景，对本申请实施例进行详细阐述。

在该应用场景中，第一设备可以为 UE，第二设备可以为 ZPD，第一网元可以为业务提供商提供的应用服务器，第二网元可以为基站。另外，第一信息可以是凭证请求信息。参考图 6 所示的流程示意图，本申请实施例提供的安全实现方法可以包括以下步骤：

步骤 601、UE 向基站发送秘钥请求信息，该秘钥请求信息用于请求与 UE 关联的 n 个零功耗设备 ZPD 的初始秘钥，其中，n 为大于或等于 1 的整数。

可选地，秘钥请求信息中可以包括 ID_{UE}、{ID_{ZP1}、…、ID_{ZPn}}、ID_{SP}、ID_{DATA}、以及第一 MAC 中的至少一项。

其中，ID_{UE} 为 UE 的标识信息，ID_{ZP1}、…、ID_{ZPn} 为与 UE 绑定的 n 个零功耗设备 ZP1 至 ZPn 分别对应的标识信息。ID_{SP} 为业务标识信息，ID_{DATA} 为数据标识信息。

另外，第一 MAC 即为秘钥请求信息的信息验证码。

可选地，UE 可以使用与基站之间协商好的秘钥 K_{AF} 或 K_{s_NAF}，对秘钥请求信息进行加密或完成性保护，得到第一 MAC。

可选地，UE 可以使用自己的私钥对秘钥请求信息的内容或部分内容进行签名，得到第一 MAC。

步骤 602、基站向 UE 发送初始秘钥信息，该初始秘钥信息中包括与 UE 关联的 n 个零功耗设备 ZPD 初始秘钥。

若 ZPD 的数量仅为一个（即 n 取值为 1），则初始秘钥信息中可以包括一个标识信息-初始秘钥对，即(ID_{ZP1}，K_{ZP1})。若 ZPD 的数量为多个（即 n 取值大于 1），则初始秘钥信息中可以包括 n 个标识信息-初始秘钥对：(ID_{ZP1}，K_{ZP1})，(ID_{ZP2}，K_{ZP2})，(ID_{ZP3}, K_{ZP3})，……，(ID_{ZPn}，K_{ZPn})。其中，ID_{ZP1} 即零功耗设备 1 的标识信息，K_{ZP1} 即零功耗设备 1 的初始秘钥，以此类推，ID_{ZPn} 即零功耗设备 n 的标识信息，K_{ZPn} 即零功耗设备 n 的初始秘钥。

可选地，初始秘钥可以是对称秘钥，第二设备的本地存储空间中也可以存储自己的初始秘钥。

可选地，当秘钥请求信息中包括业务标识信息和/或数据标识信息时，基站可以基于业务标识信息和/或数据标识信息对 n 个 ZPD 进行验证，判断 n 个 ZPD 是否具有使用该业务标识信息和/或数据标识信息对应的业务的权限。并且，只有在 n 个 ZPD 验证通过后，基站才向 UE 发送初始秘钥信息。

其中，基站可以判断本地保存的业务标识信息与秘钥请求信息中携带的 ID_{SP} 是否一致，和/或判断本地保存的数据标识信息与秘钥请求信息中携带的 ID_{DATA} 是否一致。若一致，则基站确定至少一个第二设备验证通过，至少一个第二设备具有使用该业务标识信息和/或数据标识信息对应业务的权限，若不一致，则基站确定至少一个第二设备验证失败。

可选地，基站在接收到第一设备发送的秘钥请求信息后，首先可以对 UE 的身份进行认证，以确定发送秘钥请求信息的 UE 是否是可信任的设备。进一步地，在对 UE 的身份认证通过后，基站才向 UE 发送初始秘钥信息。

可选地，基站可以基于第一 MAC，对 UE 的身份进行认证,。

在一种可能的实现方式中，若第一 MAC 是根据 UE 与基站协商的秘钥 K_{AF} 或 K_{s_NAF} 生成的，则基站可以利用该秘钥 K_{AF} 或 K_{s_NAF} 对第一 MAC 进行验证。

在另一种可能的实现方式中，若第一 MAC 时根据 UE 的私钥生成的，则基站可以使用 UE 的证书或者 UE 的公钥对第一 MAC 进行验证。

步骤 603、UE 分别与 n 个 ZPD 进行初始认证。

应理解，UE 确定 n 个 ZPD 的初始秘钥之后，可以基于每个 ZPD 的初始秘钥与每个 ZPD 进行初始认证，以确定彼此是可信的设备，防止数据泄露和窃取。

需要说明的是，UE 与每个 ZPD 之间的认证过程可以参考相关技术中的认证过程，为了简洁，此处不做赘述。

步骤 604、UE 基于业务共享秘钥 Kservice 和每个 ZPD 对应的初始秘钥，生成设备秘钥 Secret。

可选地，UE 可以直接基于业务共享秘钥 Kservice 和每个 ZPD 对应的初始秘钥，生成设备秘钥 Secret。

示例性的，若 ZPD 的数量为 1，则设备秘钥 Secret 即为 Kservice 和该 ZPD 的初始秘钥汇聚后的结果。若 ZPD 的数量包括多个，则 UE 可以将 Kservice 和每个 ZPD 的初始秘钥进行汇聚处理，得到上述设备秘钥 Secret。其中，汇聚处理可以是将多个秘钥直连处理。

可选地，UE 可以基于每个 ZPD 的初始秘钥，与该 ZPD 进行物理层安全机制的协商处理，生成各个 ZPD 对应的中间秘钥。进而，UE 可以基于业务共享秘钥 Kservice 和每个 ZPD 的中间秘钥，生成设备秘钥 Secret。

示例性的，若 ZPD 的数量为 1，则设备秘钥 Secret 即为业务共享秘钥 Kservice 和该 ZPD 的中间秘钥汇聚后的结果。若 ZPD 的数量包括多个，则 UE 可以将业务共享秘钥 Kservice 和每个 ZPD 的中间秘钥进行汇聚处理，得到上述设备秘钥 Secret。其中，汇聚处理可以是将多个秘钥直连处理。

步骤 605、UE 生成设备绑定验证码 DAC，和/或，业务验证码 SAC。其中，DAC 用于验证 UE 与 n 个 ZPD 之间的关联关系；SAC 用于验证 UE 和/或 n 个 ZPD 是否支持 ID_{SP} 指示的业务类型，和/或，UE 和/或 n 个 ZPD 是否支持 ID_{DATA} 指示的数据类型。

本申请实施例中，UE 可以基于设备秘钥 Secret，生成设备绑定验证码 DAC。示例性的，UE 可以参考公式（1）来计算 DAC。

本申请实施例中，UE 可以基于 ID_{UE}、{ID_{ZP1}、…、ID_{ZPn}}、ID_{SP}、ID_{DATA}、NONCE、COUNT 中的至少一项，生成业务验证码 SAC。

可选地，UE 可以利用其私钥对 ID_{UE}、{ID_{ZP1}、…、ID_{ZPn}}、ID_{SP}、ID_{DATA}、NONCE、COUNT 在内的至少一项信息进行签名，得到 SAC。具体计算方式可以参考公式（2），此处不做赘述。

可选地，UE 可以利用业务共享秘钥 Kservice，对 ID_{UE}、{ID_{ZP1}、…、ID_{ZPn}}、ID_{SP}、ID_{DATA}、NONCE、COUNT 中的至少一项进行加密和完整性保护，得到 SAC。具体计算方式可以参考公式（3），此处

不做赘述。

步骤 606、UE 向基站发送凭证请求信息，凭证请求信息用于请求 n 个 ZPD 的授权凭证。

本申请实施例中，凭证请求信息中可以包括 DAC 和/或 SAC，以及 ID_{UE}、{ID_{ZP1}、…、ID_{ZPn}}、ID_{SP}、ID_{DATA}、和第二 MAC 中的至少一项。

其中，第二 MAC 可以是 UE 使用自己的私钥，对凭证请求信息中其他的全部信息或部分信息进行签名处理得到。该第二 MAC 用于验证凭证请求信息的发送方是否为合法设备。

可选地，UE 可以直接向应用服务器发送凭证请求信息。

步骤 607、基站对凭证请求信息中的 DAC 进行验证。

本申请实施例中，基站可以通过 DAC 来确定 UE 与 n 个 ZPD 是否具有真实的关联关系。

具体地，基站可以基于设备秘钥 Secret，生成第一校验信息。其中，基站可以参考上述公式（1）来生成第一校验信息。若第一校验信息与凭证请求信息中的 DAC 一致，可以认为 UE 与 n 个 ZPD 之间真实存在关联关系，基站确定 DAC 验证通过。若第一校验信息与 DAC 不一致，则认为 UE 与 n 个 ZPD 之间的关联关系错误或不存在，基站确定 DAC 验证不通过。

其中，基站可以从 UE 处获取设备秘钥 Secret，也可以从其他受信任的设备（例如 UDM 网元、应用服务器等）处获取设备秘钥 Secret。基站还可以基于业务共享秘钥 Kservice 和每个第二设备的初始秘钥，生成该设备秘钥 Secret。本申请实施例对此不做限制。

步骤 608、基站在对 DAC 验证通过的情况下，向应用服务器发送凭证请求信息。

可选地，基站在确定了 UE 与 n 个 ZPD 之间真实存在关联关系之后，可以将凭证请求信息转发给 ID_{SP} 和/或 ID_{DATA} 对应的应用服务器。

步骤 609、在对 SAC 验证通过的情况下，应用服务器为 n 个 ZPD 生成授权凭证。

可以理解的是，应用服务器接收到凭证请求信息之后，通过 SAC 来验证 UE 和/或 n 个 ZPD 支持的业务类型是否是 ID_{SP} 指示的业务类型，和/或，UE 和/或 n 个 ZPD 支持的数据类型是否是 ID_{DATA} 指示的数据类型。

可选地，若 SAC 是利用 UE 的私钥对 ID_{UE}、{ID_{ZP1}、…、ID_{ZPn}}、ID_{SP}、ID_{DATA}、NONCE、COUNT 在内的至少一项信息进行签名得到，则应用服务器可以利用 UE 的公钥对 SAC 进行验证。

具体地，应用服务器可以通过 UE 的公钥对 SAC 进行验证，得到第二校验信息。若第二校验信息与凭证请求信息中携带的 ID_{UE}、{ID_{ZP1}、…、ID_{ZPn}}、ID_{SP}、ID_{DATA}、NONCE、COUNT 至少一项信息一致，则确定 SAC 验证通过。否则，确定 SAC 验证不通过。

可选地，在另一些实施例中，若 SAC 是利用业务共享秘钥 Kservice，对 ID_{UE}、{ID_{ZP1}、…、ID_{ZPn}}、ID_{SP}、ID_{DATA}、NONCE、COUNT 在内的至少一项信息进行安全运算得到，则应用服务器可以利用业务共享秘钥 Kservice，对 SAC 进行验证。

具体地，应用服务器首先可以基于业务共享秘钥 Kservice，对 ID_{UE}、{ID_{ZP1}、…、ID_{ZPn}}、ID_{SP}、ID_{DATA}、NONCE、COUNT 在内的至少一项信息进行安全运算，得到第三校验信息；其中，应用服务器可以参考上述公式（3）来生成第三校验信息。若第三校验信息与所述 SAC 一致，则应用服务器确定 SAC 验证通过。否者，确定 SAC 验证不通过。

本申请实施例中，应用服务器在对 SAC 验证通过后，可以为 n 个 ZPD 生成授权凭证。

可选地，应用服务器在生成授权凭证之前，可以为每个 ZPD 生成 RSA 累加器参数 α_{ZP}。其中，每个 ZPD 的 RSA 累加器参数 α_{ZP} 可以用于证明该 ZPD 的是否被撤销。

可选地，授权凭证中可以包括：ID_{UE}、pk_{UE}、{ID_{ZP1}、…、ID_{ZPn}}、DAC、α_{ZP1}、…、α_{ZPn}、ID_{SP}、ID_{IS}、ID_{DATA}、Sig_{skIS} 中的至少一项。

其中，pk_{UE} 为 UE 的公钥，ID_{IS} 为应用服务器 IS 的标识信息，Sig_{skIS} 是应用服务器利用自己的私钥对上述授权凭证中的其他信息进行签名得到。

示例性的，ZPD 的数量为 1 时，该 ZPD 的授权凭证可以为：$Cert_{IS->ZP}$([ID_{ZP1}, DAC], α_{ZP1}, ID_{UE}, ID_{IS}, ID_{SP}, Sig_{skIS})。ZPD 的数量大于 1 时，ZPD 授权凭证可以为：$Cert_{IS->ZPg}$([ID_{ZP1}, …, ID_{ZPn}, DAC], α_{ZP1}, …, α_{ZPn}, ID_{UE}, ID_{IS}, ID_{SP}, Sig_{skIS})。其中，α_{ZP1}, …, α_{ZPn} 分别为 n 个第二设备对应的 RSA 累加器参数。

需要说明的是，当业务标识信息 ID_{SP} 为应用服务器的 ID 时，ID_{SP} 和 ID_{IS} 相同，则应用服务器可以仅使用其中的一种来生成授权凭证。

步骤 610、应用服务器将授权凭证上传到区块链节点的存储区块。

步骤 611、应用服务器获取该授权凭证的存储位置信息，并向 UE 发送授权凭证，和/或，该授权凭证的存储位置信息。

综上所述，本申请实施例提供的安全实现方法中，UE 可以作为中间代理设备，为其关联的多个零功耗设备实现安全运算，以获得多个零功耗设备的授权凭证。也就是说，可以借用 UE 与应用服务器进行交互，以使应用服务器为多个零功耗设备生成轻量级的群组授权凭证，以便对零功耗设备的上行数据传输进行授权，避免攻击者或者伪基站恶意触发零功耗设备的上行数据传输，保证零功耗设备的上行传输数据的安全，提高零功耗设备的授权的效率。

以上结合附图详细描述了本申请的优选实施方式，但是，本申请并不限于上述实施方式中的具体细节，在本申请的技术构思范围内，可以对本申请的技术方案进行多种简单变型，这些简单变型均属于本申请的保护范围。例如，在上述具体实施方式中所描述的各个具体技术特征，在不矛盾的情况下，可以通过任何合适的方式进行组合，为了避免不必要的重复，本申请对各种可能的组合方式不再另行说明。又例如，本申请的各种不同的实施方式之间也可以进行任意组合，只要其不违背本申请的思想，其同样应当视为本申请所公开的内容。又例如，在不冲突的前提下，本申请描述的各个实施例和/或各个实施例中的技术特征可以和现有技术任意的相互组合，组合之后得到的技术方案也应落入本申请的保护范围。

还应理解，在本申请的各种方法实施例中，上述各过程的序号的大小并不意味着执行顺序的先后，各过程的执行顺序应以其功能和内在逻辑确定，而不应对本申请实施例的实施过程构成任何限定。此外，在本申请实施例中，术语“下行”、“上行”和“侧行”用于表示信号或数据的传输方向，其中，“下行”用于表示信号或数据的传输方向为从站点发送至小区的用户设备的第一方向，“上行”用于表示信号或数据的传输方向为从小区的用户设备发送至站点的第二方向，“侧行”用于表示信号或数据的传输方向为从用户设备 1 发送至用户设备 2 的第三方向。例如，“下行信号”表示该信号的传输方向为第一方向。另外，本申请实施例中，术语“和/或”，仅仅是一种描述关联对象的关联关系，表示可以存在三种关系。具体地，A 和/或 B 可以表示：单独存在 A，同时存在 A 和 B，单独存在 B 这三种情况。另外，本文中字符“/”，一般表示前后关联对象是一种“或”的关系。

图 7 是本申请实施例提供的安全实现装置 700 的结构组成示意图，应用于第一网元，如图 7 所示，所述安全实现装置 700 包括：

第一接收单元 701，被配置为接收第一信息；所述第一信息中包括设备绑定验证码 DAC，和/或，业务验证码 SAC；DAC 用于验证第一设备与至少一个第二设备之间的关联关系，SAC 用于验证所述第一设备和/或所述至少一个第二设备是否支持业务标识信息指示的业务类型，和/或，所述第一设备和/或所述至少一个第二设备是否支持数据标识信息指示的数据类型。

可选地，所述第一信息中还包括以下中的至少一项：

业务标识信息；所述业务标识信息用于指示所述第一设备和/或所述至少一个第二设备支持的业务类型；

数据标识信息；所述业务标识信息用于指示所述第一设备和/或所述至少一个第二设备支持的数据类型；

所述第一设备的标识信息；

所述至少一个第二设备中每个第二设备的标识信息；

设备秘钥 Secret；

所述第一信息对应的第一信息验证码 MAC；第一 MAC 用于验证所述第一信息的发送方是否为合法设备。

可选地，所述第一信息用于请求与所述第一设备关联的所述至少一个第二设备发放授权凭证；所述安全实现装置 700 还包括：

凭证生成单元，被配置为在对所述 DAC 和/或所述 SAC 验证通过的情况下，为所述至少一个第二设备生成授权凭证。

可选地，所述安全实现装置 700 还包括验证单元，被配置为：基于设备秘钥 Secret，生成第一校验信息；若所述第一校验信息与所述 DAC 一致，则确定所述 DAC 验证通过。

可选地，所述验证单元，还被配置为基于业务共享秘钥 Kservice，和/或，所述至少一个第二设备中每个第二设备的初始秘钥，生成所述设备秘钥 Secret，其中，所述业务共享秘钥 Kservice 为所述第一网元与所述第一设备之间的共享秘钥。

可选地，所述验证单元，还被配置为基于业务共享秘钥 Kservice，和/或，每个第二设备的初始秘钥，计算每个第二设备的中间秘钥；基于业务共享秘钥 Kservice 和/或，所述至少一个第二设备中每个第二设备的中间秘钥，生成所述设备秘钥 Secret。

可选地，所述 SAC 是利用所述第一设备的私钥对所述第一设备的标识标识信息、每个第二设备

的标识信息、业务标识信息、以及数据标识信息、随机数 NONCE、以及计数器参数 COUNT 在内的至少一项信息进行签名得到；

对应的，所述验证单元，还被配置为利用所述第一设备的公钥对所述 SAC 进行验证，得到第二校验信息；若所述第二校验信息与所述第一信息中携带的所述第一设备的标识信息、每个第二设备的标识信息、所述业务标识信息、所述数据标识信息、随机数 NONCE、以及计数器参数 COUNT 一致，则确定所述 SAC 验证通过。

可选地，所述 SAC 是利用业务共享秘钥 Kservice，对所述第一设备的标识信息、所述至少一个第二设备中每个第二设备的标识信息、所述业务标识信息、所述数据标识信息、随机数 NONCE、以及计数器参数 COUNT 中的至少一项进行安全运算得到；

对应的，所述验证单元，还被配置为基于所述业务共享秘钥 Kservice，对所述第一设备的标识信息、所述每个第二设备的标识信息、所述业务标识信息、所述数据标识信息、所述随机数 NONCE、以及所述计数器参数 COUNT 中的至少一项进行安全运算，得到第三校验信息；若所述第三校验信息与所述 SAC 一致，则确定所述 SAC 验证通过。

可选地，所述授权凭证包括以下中的至少一项：

所述第一设备的标识信息；

所述第一设备的公钥；

所述至少一个第二设备中每个第二设备的标识信息；

所述至少一个第二设备中每个第二设备的 RSA 累加器参数；

所述第一网元的标识信息；

所述第一网元的公钥；

业务标识信息；

数据标识信息；

设备绑定验证码 DAC；

所述第一网元的数字签名；所述数字签名是基于所述第一网元的私钥对所述授权凭证中其他信息进行签名得到。

可选地，所述安全实现装置 700 还包括第一发送单元，被配置为向区块链节点发送所述授权凭证；所述第一接收单元 701，还被配置为获取所述授权凭证的存储位置信息。

可选地，第一发送单元，还配置为向所述第一设备发送授权凭证，和/或，所述存储位置信息。

图 8 是本申请实施例提供的安全实现装置 800 的结构组成示意图，应用于第一设备，如图 8 所示，所述安全实现装置 800 包括：

第二发送单元 801，被配置为发送第一信息；所述第一设备与至少一个第二设备关联；所述第一信息中包括设备绑定验证码 DAC，和/或，业务验证码 SAC；DAC 用于验证第一设备与至少一个第二设备之间的关联关系，SAC 用于验证所述第一设备和/或所述至少一个第二设备是否支持业务标识信息指示的业务类型，和/或，所述第一设备和/或所述至少一个第二设备是否支持数据标识信息指示的数据类型。

可选地，所述第一信息还包括以下中的至少一项：

业务标识信息；所述业务标识信息用于指示所述第一设备和/或所述至少一个第二设备支持的业务类型；

数据标识信息；所述业务标识信息用于指示所述第一设备和/或所述至少一个第二设备支持的数据类型；

所述第一设备的标识信息；

所述至少一个第二设备中每个第二设备的标识信息；

设备秘钥 Secret；

所述第一信息对应的第一信息验证码 MAC；第一 MAC 用于验证所述第一信息的发送方是否为合法设备。

可选地，所述安全实现装置 800 还包括处理单元，被配置为基于设备秘钥 Secret，生成所述设备绑定验证码 DAC；和/或，基于第一设备的标识信息、每个第二设备的标识信息、业务标识信息、以及数据标识信息在内的至少一项，生成业务验证码 SAC。

可选地，所述处理单元，还被配置基于业务共享秘钥 Kservice，和/或，所述至少一个第二设备中每个第二设备的初始秘钥，生成所述设备秘钥 Secret；其中，所述业务共享秘钥 Kservice 为第一网元与第一设备之间的共享秘钥。

可选地，所述处理单元，还被配置为基于每个第二设备的初始秘钥，生成每个第二设备的中间秘钥；基于业务共享秘钥 Kservice，和/或，所述至少一个第二设备中每个第二设备的中间秘钥，生成所述设备秘钥 Secret。

可选地，所述第二发送单元 801，还被配置为向第二网元发送秘钥请求信息；所述秘钥请求信息用于请求与所述第一设备关联的至少一个第二设备的初始秘钥。

可选地，所述安全实现装置 800 还包括第二接收单元，被配置为接收所述第二网元发送的初始秘钥信息；所述初始秘钥信息中包括每个第二设备的初始秘钥。

可选地，所述秘钥请求信息还包括以下中的至少一项：

第一设备的标识信息；

至少一个第二设备中每个第二设备的标识信息；

业务标识信息；

数据标识信息；

所述秘钥请求信息对应的第二 MAC；所述第二 MAC 用于验证所述秘钥请求信息的发送方是否为合法设备。

可选地，所述处理单元，还被配置为利用所述第一设备的私钥对所述第一设备的标识信息、所述每个第二设备的标识信息、所述业务标识信息、所述数据标识信息、随机数 NONCE、以及计数器参数 COUNT 在内的至少一项信息进行签名，得到所述 SAC。

可选地，所述处理单元，还被配置为基于业务共享秘钥 Kservice，对所述第一设备的标识信息、所述每个第二设备的标识信息、所述业务标识信息、所述数据标识信息、随机数 NONCE、以及计数器参数 COUNT 中的至少一项进行安全运算，生成所述 SAC。

可选地，所述第一信息用于请求与所述第一设备关联的至少一个第二设备的授权凭证。

本领域技术人员应当理解，本申请实施例的上述安全实现装置的相关描述可以参照本申请实施例的安全实现方法的相关描述进行理解。

图 9 是本申请实施例提供的一种通信设备 900 示意性结构图。该通信设备可以是第一网元，也可以是第一设备。图 9 所示的通信设备 900 包括处理器 910，处理器 910 可以从存储器中调用并运行计算机程序，以实现本申请实施例中的方法。

可选地，如图 9 所示，通信设备 900 还可以包括存储器 920。其中，处理器 910 可以从存储器 920 中调用并运行计算机程序，以实现本申请实施例中的方法。

其中，存储器 920 可以是独立于处理器 910 的一个单独的器件，也可以集成在处理器 910 中。

可选地，如图 9 所示，通信设备 900 还可以包括收发器 930，处理器 910 可以控制该收发器 930 与其他设备进行通信，具体地，可以向其他设备发送信息或数据，或接收其他设备发送的信息或数据。

其中，收发器 930 可以包括发射机和接收机。收发器 930 还可以进一步包括天线，天线的数量可以为一个或多个。

可选地，该通信设备 900 具体可为本申请实施例的第一网元，并且该通信设备 900 可以实现本申请实施例的各个方法中由第一网元实现的相应流程，为了简洁，在此不再赘述。

可选地，该通信设备 900 具体可为本申请实施例的第一设备，并且该通信设备 1800 可以实现本申请实施例的各个方法中由第一设备实现的相应流程，为了简洁，在此不再赘述。

图 10 是本申请实施例的芯片的示意性结构图。图 10 所示的芯片 1000 包括处理器 1010，处理器 1010 可以从存储器中调用并运行计算机程序，以实现本申请实施例中的方法。

可选地，如图 10 所示，芯片 1900 还可以包括存储器 1020。其中，处理器 1010 可以从存储器 1020 中调用并运行计算机程序，以实现本申请实施例中的方法。

其中，存储器 1020 可以是独立于处理器 1010 的一个单独的器件，也可以集成在处理器 100 中。

可选地，该芯片 1000 还可以包括输入接口 1030。其中，处理器 1010 可以控制该输入接口 1030 与其他设备或芯片进行通信，具体地，可以获取其他设备或芯片发送的信息或数据。

可选地，该芯片 1000 还可以包括输出接口 1040。其中，处理器 1010 可以控制该输出接口 1040 与其他设备或芯片进行通信，具体地，可以向其他设备或芯片输出信息或数据。

可选地，该芯片可应用于本申请实施例中的第一网元，并且该芯片可以实现本申请实施例的各个方法中由第一网元实现的相应流程，为了简洁，在此不再赘述。

可选地，该芯片可应用于本申请实施例中的第一设备，并且该芯片可以实现本申请实施例的各个方法中由第一设备实现的相应流程，为了简洁，在此不再赘述。

应理解，本申请实施例提到的芯片还可以称为系统级芯片，系统芯片，芯片系统或片上系统芯片等。

图 11 是本申请实施例提供的一种通信系统 1100 的示意性框图。如图 11 所示，该通信系统 1100 包括第一设备 1110 和第一网元 1120。

其中，该第一设备 1110 可以用于实现上述方法中由第一设备实现的相应的功能，以及该第一网元 1120 可以用于实现上述方法中由第一网元实现的相应的功能为了简洁，在此不再赘述。

应理解，本申请实施例的处理器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，上述方法实施例的各步骤可以通过处理器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申请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。结合本申请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，处理器读取存储器中的信息，结合其硬件完成上述方法的步骤。

可以理解，本申请实施例中的存储器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，DDR SDRAM）、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，DR RAM）。应注意，本文描述的系统和方法的存储器旨在包括但不限于这些和任意其它适合类型的存储器。

应理解，上述存储器为示例性但不是限制性说明，例如，本申请实施例中的存储器还可以是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，DDR SDRAM）、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（synch link DRAM，SLDRAM）以及直接内存总线随机存取存储器（Direct Rambus RAM，DR RAM）等等。也就是说，本申请实施例中的存储器旨在包括但不限于这些和任意其它适合类型的存储器。

本申请实施例还提供了一种计算机可读存储介质，用于存储计算机程序。

可选的，该计算机可读存储介质可应用于本申请实施例中的第一网元，并且该计算机程序使得计算机执行本申请实施例的各个方法中由第一网元实现的相应流程，为了简洁，在此不再赘述。

可选地，该计算机可读存储介质可应用于本申请实施例中的第一设备，并且该计算机程序使得计算机执行本申请实施例的各个方法中由第一设备实现的相应流程，为了简洁，在此不再赘述。

本申请实施例还提供了一种计算机程序产品，包括计算机程序指令。

可选的，该计算机程序产品可应用于本申请实施例中的第一网元，并且该计算机程序指令使得计算机执行本申请实施例的各个方法中由第一网元实现的相应流程，为了简洁，在此不再赘述。

可选地，该计算机程序产品可应用于本申请实施例中的第一设备，并且该计算机程序指令使得计算机执行本申请实施例的各个方法中由第一设备实现的相应流程，为了简洁，在此不再赘述。

本申请实施例还提供了一种计算机程序。

可选的，该计算机程序可应用于本申请实施例中的第一网元，当该计算机程序在计算机上运行时，使得计算机执行本申请实施例的各个方法中由第一网元实现的相应流程，为了简洁，在此不再赘述。

可选地，该计算机程序可应用于本申请实施例中的第一设备，当该计算机程序在计算机上运行时，使得计算机执行本申请实施例的各个方法中由第一设备实现的相应流程，为了简洁，在此不再赘述。

本领域普通技术人员可以意识到，结合本文中所公开的实施例描述的各示例的单元及算法步骤，能够以电子硬件、或者计算机软件和电子硬件的结合来实现。这些功能究竟以硬件还是软件方式来执行，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申请的范围。

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，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。

所述功能如果以软件功能单元的形式实现并作为独立的产品销售或使用时，可以存储在一个计算机可读取存储介质中。基于这样的理解，本申请的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的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（Read-Only Memory，）ROM、随机存取存储器（Random Access Memory，RAM）、磁碟或者光盘等各种可以存储程序代码的介质。

以上所述，仅为本申请的具体实施方式，但本申请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申请揭露的技术范围内，可轻易想到变化或替换，都应涵盖在本申请的保护范围之内。因此，本申请的保护范围应所述以权利要求的保护范围为准。

权利要求书

1、一种安全实现方法，所述方法包括:

第一网元接收第一信息；所述第一信息包括设备绑定验证码 DAC，和/或，业务验证码 SAC；其中，DAC 用于验证第一设备与至少一个第二设备之间的关联关系，SAC 用于验证所述第一设备和/或所述至少一个第二设备是否支持业务标识信息指示的业务类型，和/或，所述第一设备和/或所述至少一个第二设备是否支持数据标识信息指示的数据类型。

2、根据权利要求 1 所述的方法，其中，所述第一信息中还包括以下中的至少一项:

业务标识信息；所述业务标识信息用于指示所述第一设备和/或所述至少一个第二设备支持的业务类型；

数据标识信息；所述业务标识信息用于指示所述第一设备和/或所述至少一个第二设备支持的数据类型；

所述第一设备的标识信息；

所述至少一个第二设备中每个第二设备的标识信息；

设备秘钥 Secret；

所述第一信息对应的第一信息验证码 MAC；第一 MAC 用于验证所述第一信息的发送方是否为合法设备。

3、根据权利要求 1 或 2 所述的方法，其中，所述第一信息用于请求与所述第一设备关联的所述至少一个第二设备发放授权凭证；

所述方法还包括:

在对所述 DAC 和/或所述 SAC 验证通过的情况下，所述第一网元为所述至少一个第二设备生成授权凭证。

4、根据权利要求 3 所述的方法，其中，还包括:

所述第一网元基于设备秘钥 Secret，生成第一校验信息；

若所述第一校验信息与所述 DAC 一致，则所述第一网元确定所述 DAC 验证通过。

5、根据权利要求 4 所述的方法，其中，所述第一网元基于设备秘钥 Secret，生成第一校验信息之前，还包括:

所述第一网元基于业务共享秘钥 Kservice，和/或，所述至少一个第二设备中每个第二设备的初始秘钥，生成所述设备秘钥 Secret；

其中，所述业务共享秘钥 Kservice 为所述第一网元与所述第一设备之间的共享秘钥。

6、根据权利要求 5 所述的方法，其中，所述第一网元基于业务共享秘钥 Kservice，和/或，每个第二设备的初始秘钥，计算所述设备秘钥 Secret，包括:

所述第一网元基于每个第二设备的初始秘钥，计算每个第二设备的中间秘钥；

所述第一网元基于所述业务共享秘钥 Kservice，和/或，所述至少一个第二设备中每个第二设备的中间秘钥，生成所述设备秘钥 Secret。

7、根据权利要求 3-6 任一项所述的方法，其中，所述 SAC 基于所述第一设备的私钥对所述第一设备的标识标识信息、每个第二设备的标识信息、业务标识信息、数据标识信息、随机数 NONCE、以及计数器参数 COUNT 在内的至少一项信息进行签名得到；

对应的，所述方法还包括:

所述第一网元利用所述第一设备的公钥对所述 SAC 进行验证，得到第二校验信息；

若所述第二校验信息与所述第一信息中携带的所述第一设备的标识信息、每个第二设备的标识信息、所述业务标识信息、所述数据标识信息、所述随机数 NONCE、以及所述计数器参数 COUNT 一致，则所述第一网元确定所述 SAC 验证通过。

8、根据权利要求 3-6 任一项所述的方法，其中，所述 SAC 是基于业务共享秘钥 Kservice，对所述第一设备的标识信息、所述至少一个第二设备中每个第二设备的标识信息、所述业务标识信息、所述数据标识信息、随机数 NONCE、以及计数器参数 COUNT 中的至少一项进行安全运算得到；

对应的，所述方法还包括:

所述第一网元基于所述业务共享秘钥 Kservice，对所述第一设备的标识信息、所述每个第二设备的标识信息、所述业务标识信息、所述数据标识信息、随机数 NONCE、以及计数器参数 COUNT

中的至少一项进行安全运算，得到第三校验信息；

若所述第三校验信息与所述 SAC 一致，则所述第一网元确定所述 SAC 验证通过。

9、根据权利要求 3-8 任一项所述的方法，其中，所述授权凭证包括以下中的至少一项：

所述第一设备的标识信息；

所述第一设备的公钥；

所述至少一个第二设备中每个第二设备的标识信息；

所述至少一个第二设备中每个第二设备的 RSA 累加器参数；

所述第一网元的标识信息；

所述第一网元的公钥；

业务标识信息；

数据标识信息；

设备绑定验证码 DAC；

所述第一网元的数字签名；所述数字签名是基于所述第一网元的私钥对所述授权凭证中其他信息进行签名得到。

10、根据权利要求 3-9 任一项所述的方法，其中，还包括：

所述第一网元向区块链节点发送所述授权凭证；

所述第一网元获取所述授权凭证的存储位置信息。

11、根据权利要求 10 所述的方法，其中，还包括：

所述第一网元向所述第一设备发送所述授权凭证，和/或，所述存储位置信息。

12、一种安全实现方法，所述方法包括：

第一设备发送第一信息；所述第一设备与至少一个第二设备关联；所述第一信息中包括设备绑定验证码 DAC，和/或，业务验证码 SAC；DAC 用于验证所述第一设备与所述至少一个第二设备之间的关联关系，SAC 用于验证所述第一设备和/或所述至少一个第二设备是否支持业务标识信息指示的业务类型，和/或，所述第一设备和/或所述至少一个第二设备是否支持数据标识信息指示的数据类型。

13、根据权利要求 12 所述的方法，其中，所述第一信息还包括以下中的至少一项：

业务标识信息；所述业务标识信息用于指示所述第一设备和/或所述至少一个第二设备支持的业务类型；

数据标识信息；所述业务标识信息用于指示所述第一设备和/或所述至少一个第二设备支持的数据类型；

所述第一设备的标识信息；

所述至少一个第二设备中每个第二设备的标识信息；

设备秘钥 Secret；

所述第一信息对应的第一信息验证码 MAC；第一 MAC 用于验证所述第一信息的发送方是否为合法设备。

14、根据权利要求 12 或 13 所述的方法，其中，所述第一设备发送第一信息之前，还包括：

所述第一设备基于设备秘钥 Secret，生成 DAC；

和/或，

所述第一设备基于第一设备的标识信息、每个第二设备的标识信息、业务标识信息、以及数据标识信息、随机数 NONCE、以及计数器参数 COUNT 在内的至少一项，生成 SAC。

15、根据权利要求 14 所述的方法，其中，所述第一设备基于设备秘钥 Secret，生成 DAC 之前，还包括：

所述第一设备基于业务共享秘钥 Kservice，和/或，所述至少一个第二设备中每个第二设备的初始秘钥，计算所述设备秘钥 Secret；

其中，所述业务共享秘钥 Kservice 为所述第一网元与所述第一设备之间的共享秘钥。

16、根据权利要求 14 所述的方法，其中，所述第一设备基于业务共享秘钥 Kservice，和/或，所述至少一个第二设备中每个第二设备的标识信息，生成所述设备秘钥 Secret，包括：

所述第一设备基于每个第二设备的初始秘钥，生成每个第二设备的中间秘钥；

所述第一设备基于业务共享秘钥 Kservice，和/或，所述至少一个第二设备中每个第二设备的中间秘钥，生成所述设备秘钥 Secret。

17、根据权利要求 15 或 16 所述的方法，其中，所述第一设备基于所述至少一个第二设备中每

个第二设备的标识信息，生成所述设备秘钥 Secret 之前，还包括:

所述第一设备向第二网元发送秘钥请求信息；所述秘钥请求信息用于请求与所述第一设备关联的至少一个第二设备的初始秘钥。

18、根据权利要求 17 所述的方法，其中，还包括:

所述第一设备接收所述秘第二网元发送的初始秘钥信息；所述初始秘钥信息中包括每个第二设备的初始秘钥。

19、根据权利要求 17 或 18 所述的方法，其中，所述秘钥请求信息还包括以下中的至少一项:

第一设备的标识信息;

至少一个第二设备中每个第二设备的标识信息;

业务标识信息;

数据标识信息;

所述秘钥请求信息对应的第二 MAC；所述第二 MAC 用于验证所述秘钥请求信息的发送方是否为合法设备。

20、根据权利要求 14-19 任一项所述的方法，其中，所述第一设备基于第一设备的标识信息、每个第二设备的标识信息、业务标识信息、数据标识信息、随机数 NONCE、以及计数器参数 COUNT 在内的至少一项，生成 SAC，包括:

所述第一设备利用其私钥对所述第一设备的标识信息、所述每个第二设备的标识信息、所述业务标识信息、所述数据标识信息、随机数 NONCE、以及计数器参数 COUNT 在内的至少一项信息进行签名，得到所述 SAC。

21、根据权利要求 14-19 任一项所述的方法，其中，所述第一设备基于第一设备的标识信息、每个第二设备的标识信息、业务标识信息、数据标识信息、随机数 NONCE、以及计数器参数 COUNT 在内的至少一项，生成 SAC，包括:

所述第一设备基于业务共享秘钥 Kservice，对所述第一设备的标识信息、所述每个第二设备的标识信息、所述业务标识信息、所述数据标识信息、随机数 NONCE、以及计数器参数 COUNT 中的至少一项进行安全运算，生成所述 SAC。

22、根据权利要求 12-21 任一项所述的方法，其中，所述第一信息用于请求与所述第一设备关联的至少一个第二设备的授权凭证。

23、一种安全实现装置，应用于第一网元，包括:

第一接收单元，被配置为接收第一信息；所述第一信息中包括设备绑定验证码 DAC，和/或，业务验证码 SAC；DAC 用于验证第一设备与至少一个第二设备之间的关联关系，SAC 用于验证所述第一设备和/或所述至少一个第二设备是否支持业务标识信息指示的业务类型，和/或，所述第一设备和/或所述至少一个第二设备是否支持数据标识信息指示的数据类型。

24、一种安全实现装置，应用于第一设备，所述第一设备与至少一个第二设备关联；包括:

第二发送单元，被配置为发送第一信息；所述第一信息中包括设备绑定验证码 DAC，和/或，业务验证码 SAC；DAC 用于验证所述第一设备与所述至少一个第二设备之间的关联关系，SAC 用于验证所述第一设备和/或所述至少一个第二设备是否支持业务标识信息指示的业务类型，和/或，所述第一设备和/或所述至少一个第二设备是否支持数据标识信息指示的数据类型。

25、一种第一网元，包括：处理器和存储器，该存储器用于存储计算机程序，所述处理器用于调用并运行所述存储器中存储的计算机程序，执行如权利要求 1 至 11 中任一项所述的方法。

26、一种第一设备，包括：处理器和存储器，该存储器用于存储计算机程序，所述处理器用于调用并运行所述存储器中存储的计算机程序，执行如权利要求 12 至 22 中任一项所述的方法。

27、一种芯片，包括：处理器，用于从存储器中调用并运行计算机程序，使得安装有所述芯片的设备执行如权利要求 1 至 11 中任一项所述的方法。

28、一种芯片，包括：处理器，用于从存储器中调用并运行计算机程序，使得安装有所述芯片的设备执行如权利要求 12 至 22 中任一项所述的方法。

29、一种计算机可读存储介质，用于存储计算机程序，所述计算机程序使得计算机执行如权利要求 1 至 11 中任一项所述的方法。

30、一种计算机可读存储介质，用于存储计算机程序，所述计算机程序使得计算机执行如权利要求 12 至 22 中任一项所述的方法。

31、一种计算机程序产品，包括计算机程序指令，该计算机程序指令使得计算机执行如权利要求 1 至 11 中任一项所述的方法。

32、一种计算机程序产品，包括计算机程序指令，该计算机程序指令使得计算机执行如权利要求 12 至 22 中任一项所述的方法。

33、一种计算机程序，所述计算机程序使得计算机执行如权利要求 1 至 11 中任一项所述的方法。

34、一种计算机程序，所述计算机程序使得计算机执行如权利要求 12 至 22 中任一项所述的方法。

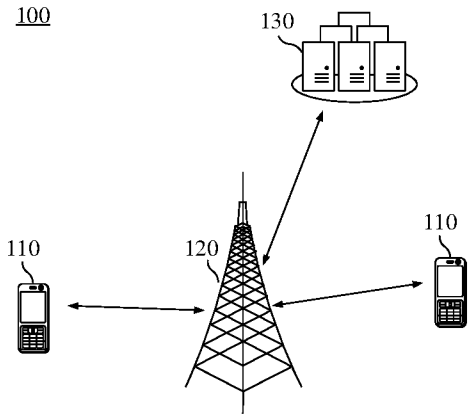
100
130
110
120
110

图 1

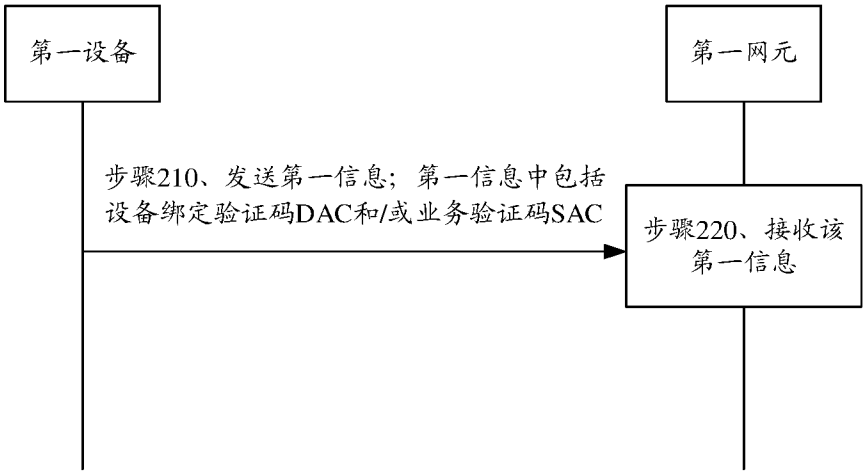
第一设备
第一网元
步骤210、发送第一信息；第一信息中包括设备绑定验证码DAC和/或业务验证码SAC
步骤220、接收该第一信息

图 2

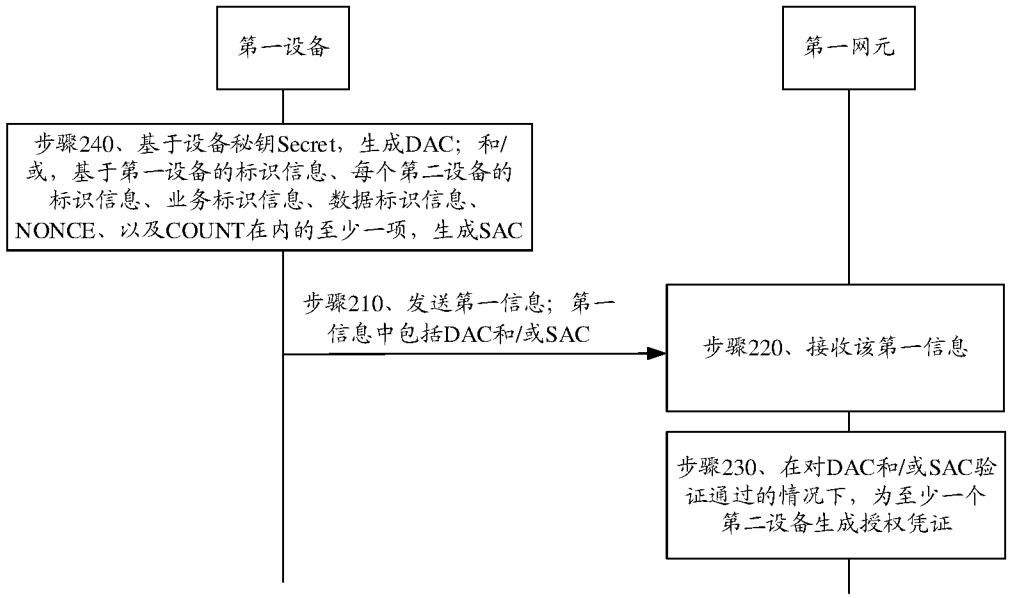
第一设备
第一网元
步骤240、基于设备秘钥Secret，生成DAC；和/或，基于第一设备的标识信息、每个第二设备的标识信息、业务标识信息、数据标识信息、NONCE、以及COUNT在内的至少一项，生成SAC
步骤210、发送第一信息；第一信息中包括DAC和/或SAC
步骤220、接收该第一信息
步骤230、在对DAC和/或SAC验证通过的情况下，为至少一个第二设备生成授权凭证

图 3

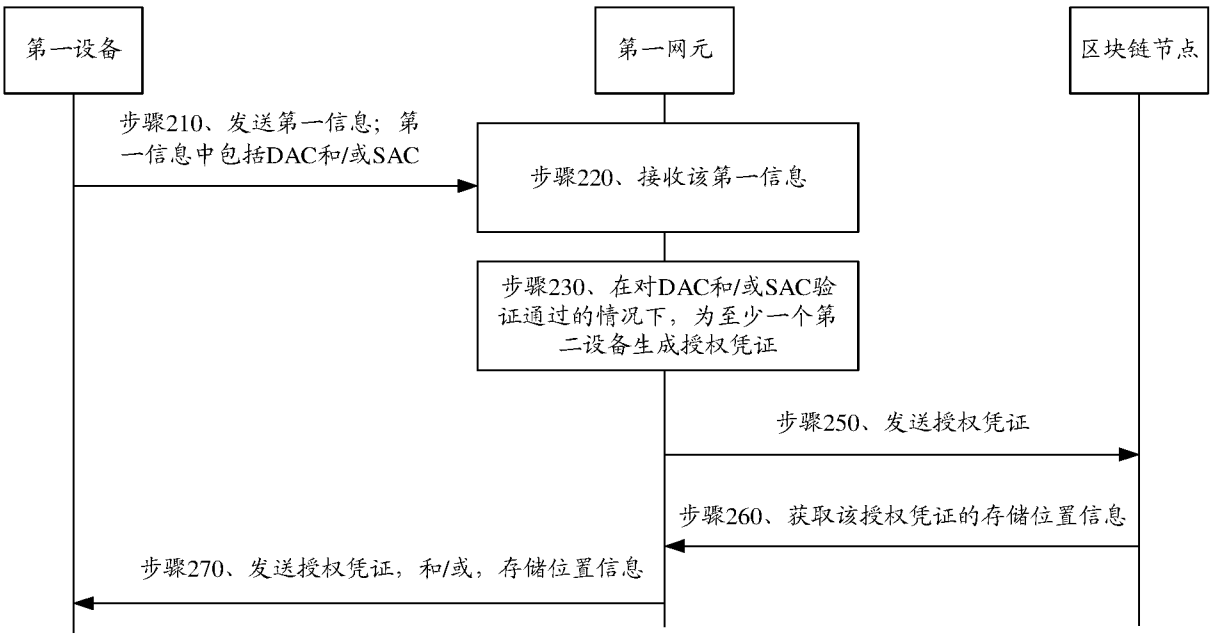
第一设备
第一网元
区块链节点
步骤210、发送第一信息；第一信息中包括DAC和/或SAC
步骤220、接收该第一信息
步骤230、在对DAC和/或SAC验证通过的情况下，为至少一个第二设备生成授权凭证
步骤250、发送授权凭证
步骤260、获取该授权凭证的存储位置信息
步骤270、发送授权凭证，和/或，存储位置信息

图 4

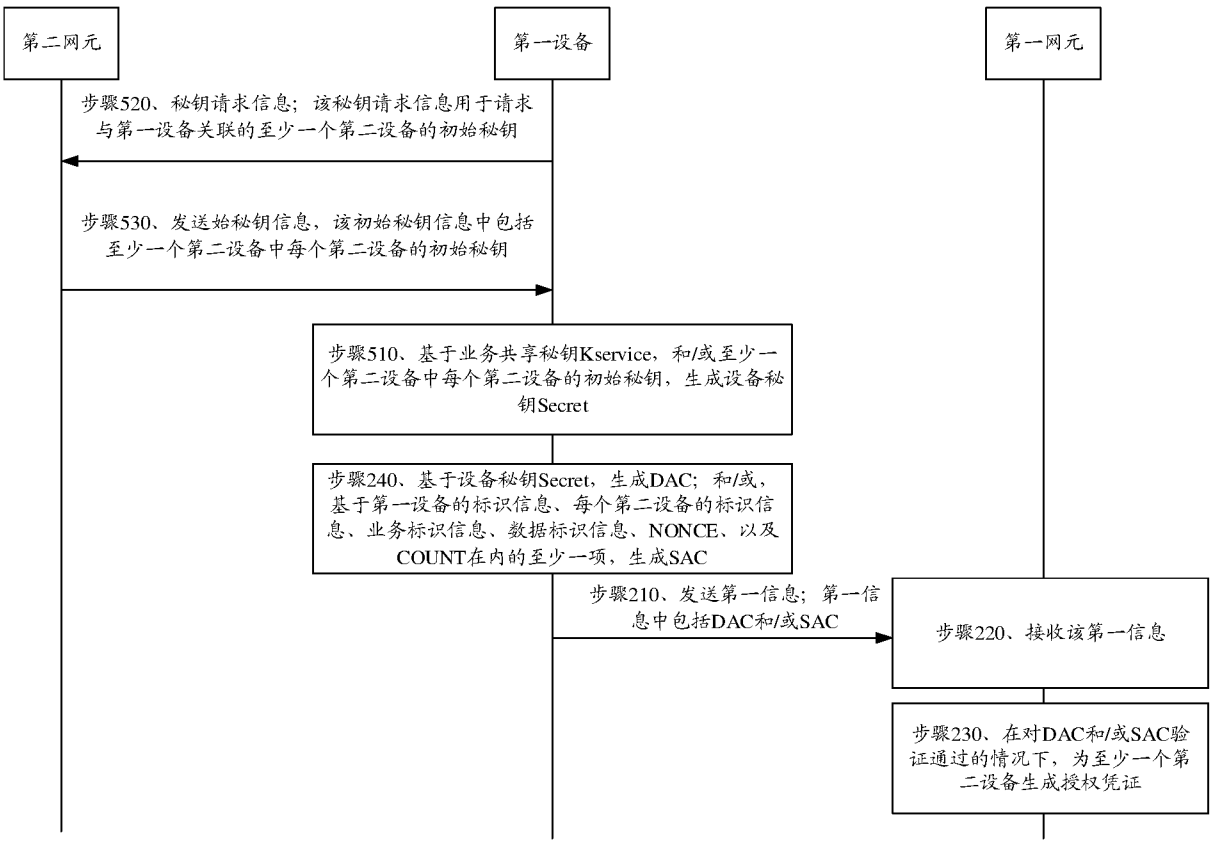
第二网元
第一设备
第一网元
步骤520、秘钥请求信息；该秘钥请求信息用于请求与第一设备关联的至少一个第二设备的初始秘钥
步骤530、发送始秘钥信息，该初始秘钥信息中包括至少一个第二设备中每个第二设备的初始秘钥
步骤510、基于业务共享秘钥Kservice，和/或至少一个第二设备中每个第二设备的初始秘钥，生成设备秘钥Secret
步骤240、基于设备秘钥Secret，生成DAC；和/或，基于第一设备的标识信息、每个第二设备的标识信息、业务标识信息、数据标识信息、NONCE、以及COUNT在内的至少一项，生成SAC
步骤210、发送第一信息；第一信息中包括DAC和/或SAC
步骤220、接收该第一信息
步骤230、在对DAC和/或SAC验证通过的情况下，为至少一个第二设备生成授权凭证

图 5

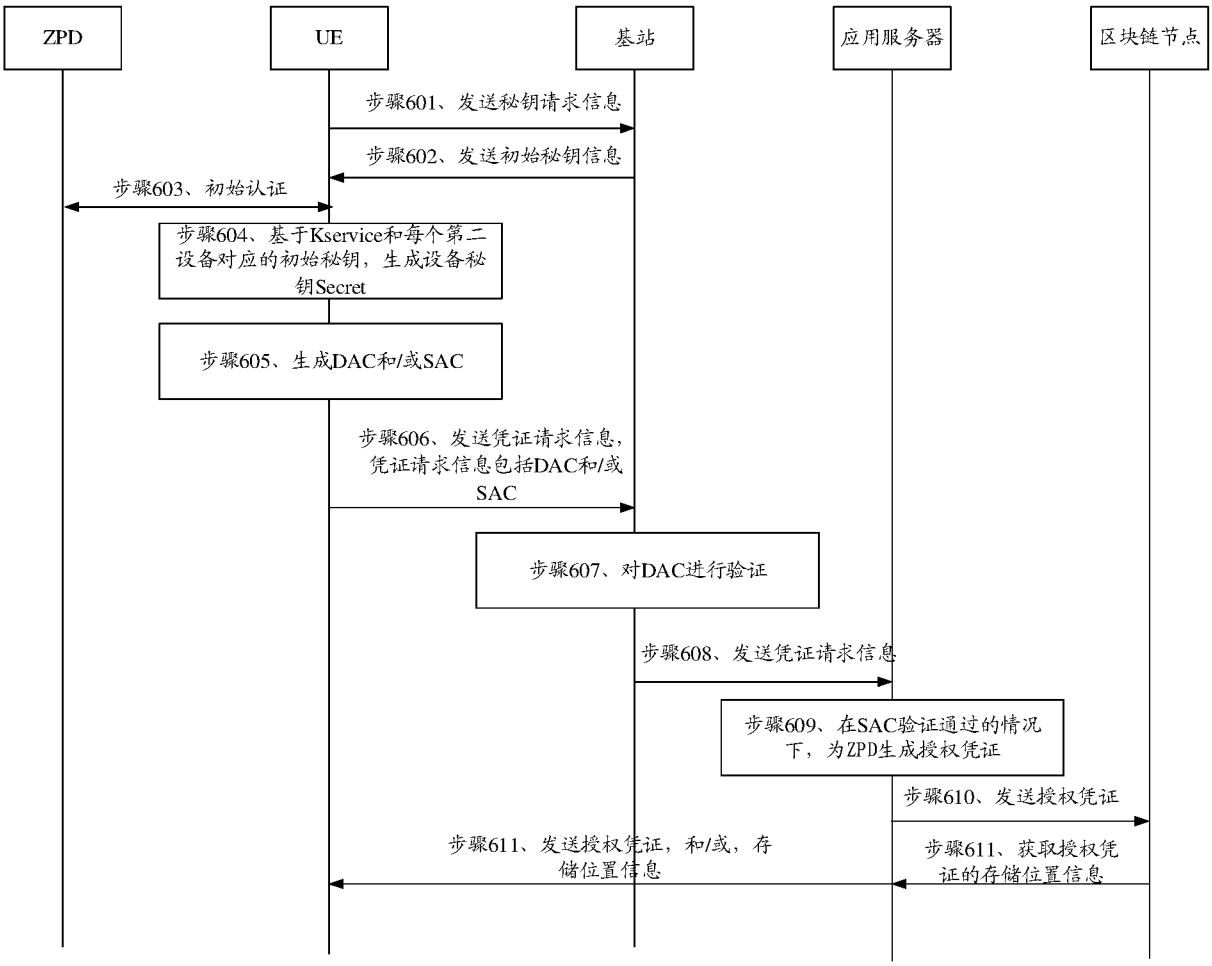
ZPD
UE
基站
应用服务器
区块链节点
步骤601、发送秘钥请求信息
步骤602、发送初始秘钥信息
步骤603、初始认证
步骤604、基于Kservice和每个第二设备对应的初始秘钥，生成设备秘钥Secret
步骤605、生成DAC和/或SAC
步骤606、发送凭证请求信息，凭证请求信息包括DAC和/或SAC
步骤607、对DAC进行验证
步骤608、发送凭证请求信息
步骤609、在SAC验证通过的情况下，为ZPD生成授权凭证
步骤610、发送授权凭证
步骤611、发送授权凭证，和/或，存储位置信息
步骤611、获取授权凭证的存储位置信息

图 6

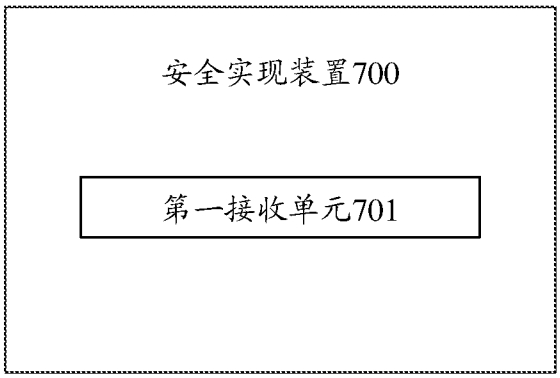
安全实现装置700
第一接收单元701

图 7

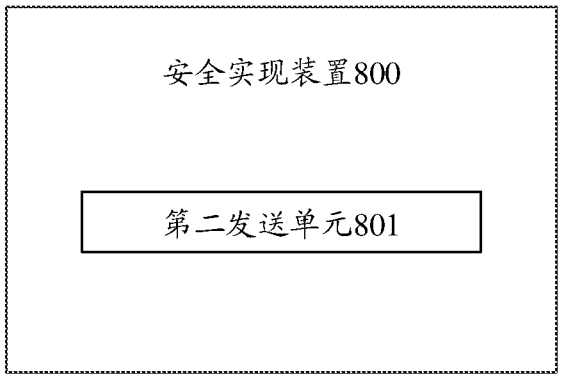
安全实现装置800
第二发送单元801

图 8

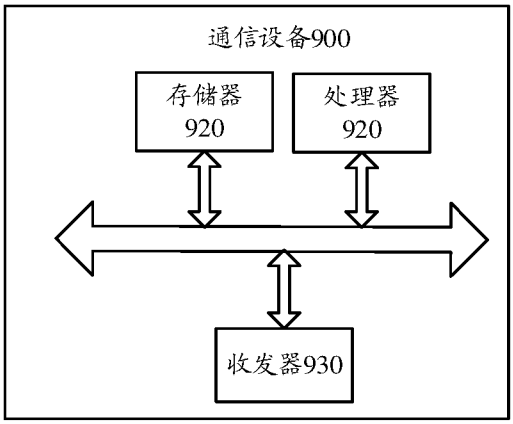
通信设备900
存储器
920
处理器
920
收发器930

图 9

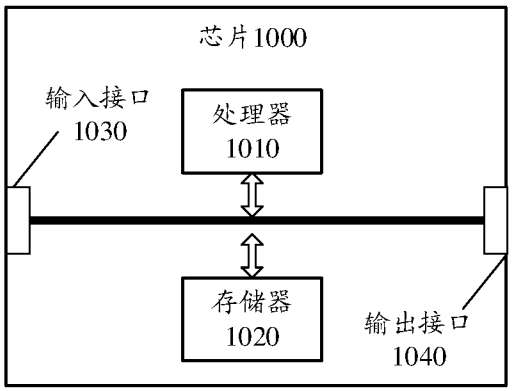
芯片1000
输入接口
1030
处理器
1010
存储器
1020
输出接口
1040

图 10

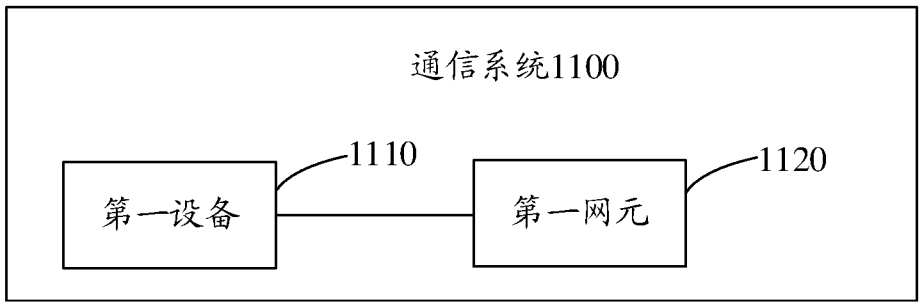
通信系统1100
1110
第一设备
1120
第一网元

图 11

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2022/083170

A. CLASSIFICATION OF SUBJECT MATTER

H04W 12/06(2021.01)i; H04L 9/32(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)

H04W; H4Q; H04L

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)

CNPAT, CNKI, WPI, EPODOC, 3GPP: 验证码, 验证, 关联, 业务类型, 数据类型, 服务类型, 授权, DAC, SAC, authentication code, verify, association, data type, service type, authenticate, authorize

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2019335332 A1 (HUAWEI TECHNOLOGIES CO., LTD.) 31 October 2019 (2019-10-31) description, paragraphs [0138]-[0287], and figures 1-6	1-34
A	CN 113407910 A (BEIJING HUAWEI DIGITAL TECHNOLOGY CO., LTD.) 17 September 2021 (2021-09-17) entire document	1-34
A	CN 101084643 A (EMUE HOLDINGS PTY LTD.) 05 December 2007 (2007-12-05) entire document	1-34
A	US 2016285633 A1 (YAHOO!, INC.) 29 September 2016 (2016-09-29) entire document	1-34
A	ERICSSON. "Editorials and Minor Clarifications for Clause 13.2" *3GPP TSG-SA WG3 Meeting #94 S3-190090,* Vol. , No. , 01 February 2019 (2019-02-01), ISSN: , entire document	1-34

☐ 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
18 October 2022	**26 October 2022**
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/CN2022/083170

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
US 2019335332 A1	31 October 2019	WO 2018126452 A1	12 July 2018
		EP 3849227 A1	14 July 2021
		CN 109716810 A	03 May 2019
		EP 3557898 A1	23 October 2019
		WO 2018126534 A1	12 July 2018
CN 113407910 A	17 September 2021	None	
CN 101084643 A	05 December 2007	CA 2591968 A1	29 June 2006
		NZ 550381 A	29 April 2011
		WO 2006066322 A1	29 June 2006
		MX 2007007511 A	08 October 2007
		JP 2008524727 A	10 July 2008
		BR PI0519184 A2	30 December 2008
		EP 1829281 A1	05 September 2007
		AU 2005318933 A1	16 November 2006
		US 2007088952 A1	19 April 2007
US 2016285633 A1	29 September 2016	US 2018159850 A1	07 June 2018
		US 2020112559 A1	09 April 2020

国际检索报告

国际申请号
PCT/CN2022/083170

A. 主题的分类

H04W 12/06(2021.01)i; H04L 9/32(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)

H04W; H4Q; H04L

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））

CNPAT,CNKI,WPI,EPODOC,3GPP：验证码，验证，关联，业务类型，数据类型，服务类型，授权，DAC，SAC，authentication code, verify, association, data type, service type, authenticate, authorize

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	US 2019335332 A1 (HUAWEI TECHNOLOGIES CO，. LTD.) 2019年10月31日 (2019-10-31) 说明书第[0138]-[0287]段，图1-6	1-34
A	CN 113407910 A (北京华为数字技术有限公司) 2021年9月17日 (2021-09-17) 全文	1-34
A	CN 101084643 A (EMUE控股集团公司) 2007年12月5日 (2007-12-05) 全文	1-34
A	US 2016285633 A1 (YAHOO!， INC.) 2016年9月29日 (2016-09-29) 全文	1-34
A	ERICSSON. "Editorials and minor clarifications for clause 13.2" 3GPP TSG-SA WG3 Meeting #94 S3-190090, 第卷，第期，2019年2月1日 (2019-02-01), ISSN：, 全文	1-34

☐ 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
2022年10月18日	2022年10月26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	受权官员 付圆媛 电话号码 86-(10)-53961775

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2022/083170

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)
US	2019335332	A1	2019年10月31日	WO	2018126452	A1	2018年7月12日
				EP	3849227	A1	2021年7月14日
				CN	109716810	A	2019年5月3日
				EP	3557898	A1	2019年10月23日
				WO	2018126534	A1	2018年7月12日
CN	113407910	A	2021年9月17日		无		
CN	101084643	A	2007年12月5日	CA	2591968	A1	2006年6月29日
				NZ	550381	A	2011年4月29日
				WO	2006066322	A1	2006年6月29日
				MX	2007007511	A	2007年10月8日
				JP	2008524727	A	2008年7月10日
				BR	PI0519184	A2	2008年12月30日
				EP	1829281	A1	2007年9月5日
				AU	2005318933	A1	2006年11月16日
				US	2007088952	A1	2007年4月19日
US	2016285633	A1	2016年9月29日	US	2018159850	A1	2018年6月7日
				US	2020112559	A1	2020年4月9日