(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
2024 年 10 月 3 日 (03.10.2024)

WIPO | PCT

(10) 国际公布号
WO 2024/199161 A1

(51) 国际专利分类号:
H04W 12/06 (2021.01)

(21) 国际申请号: PCT/CN2024/083454

(22) 国际申请日: 2024 年 3 月 25 日 (25.03.2024)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202310350033.8 2023年3月31日 (31.03.2023) CN

(71) 申请人:维沃移动通信有限公司(**VIVO MOBILE COMMUNICATION CO., LTD.**) [CN/CN]; 中国广东省东莞市长安镇维沃路 1 号, Guangdong 523863 (CN)。

(72) 发明人:郑倩(**ZHENG, Qian**); 中国广东省东莞市长安镇维沃路1号, Guangdong 523863 (CN)。 杨晓东(**YANG, Xiaodong**); 中国广东省东莞市长安镇维沃路1号, Guangdong 523863 (CN)。

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

(81) 指定国(除另有指明，要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN,

(54) **Title:** AUTHENTICATION METHOD, AUTHENTICATION APPARATUS, COMMUNICATION DEVICE AND READABLE STORAGE MEDIUM

(54) 发明名称: 鉴权方法、鉴权装置、通信设备及可读存储介质

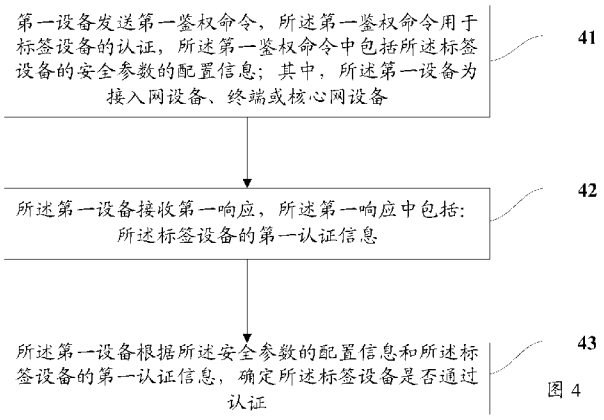

图 4

41 A first device sends a first authentication command, wherein the first authentication command is used for authorizing a tag device, the first authentication command comprises configuration information of a security parameter of the tag device, and the first device is an access network device, a terminal or a core network device

42 The first device receives a first response, wherein the first response comprises first authorization information of the tag device

43 The first device determines, according to the configuration information of the security parameter and the first authorization information of the tag device, whether the tag device is authorized

(57) **Abstract:** The present application belongs to the technical field of wireless communications. Disclosed are an authentication method, an authentication apparatus, a communication device and a readable storage medium. The authentication method for a tag device in the embodiments of the present application comprises: a first device sending a first authentication command, wherein the first authentication command is used for authorizing a tag device, the first authentication command comprises configuration information of a security parameter of the tag device, and the first device is an access network device, a terminal or a core network device; the first

WO 2024/199161 A1

[见续页]

MU, 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, CV, 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, ME, 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))。

device receiving a first response, wherein the first response comprises first authorization information of the tag device; and the first device determining, according to the configuration information of the security parameter and the first authorization information of the tag device, whether the tag device is authorized.

(57) 摘要: 本申请公开了一种鉴权方法、鉴权装置、通信设备及可读存储介质，属于无线通信技术领域，本申请实施例的标签设备的鉴权方法包括：第一设备发送第一鉴权命令，所述第一鉴权命令用于标签设备的认证，所述第一鉴权命令中包括所述标签设备的安全参数的配置信息；其中，所述第一设备为接入网设备、终端或核心网设备；所述第一设备接收第一响应，所述第一响应中包括：所述标签设备的第一认证信息；所述第一设备根据所述安全参数的配置信息和所述标签设备的第一认证信息，确定所述标签设备是否通过认证。

鉴权方法、鉴权装置、通信设备及可读存储介质

相关申请的交叉引用

本申请主张在2023年03月31日在中国提交的中国专利申请No. 202310350033.8的优先权，其全部内容通过引用包含于此。

技术领域

本申请属于无线通信技术领域，具体涉及一种鉴权方法、鉴权装置、通信设备及可读存储介质。

背景技术

未来第三代合作伙伴计划（3rd Generation Partnership Project，3GPP）相关的通信系统中将支持一种全新的物联网（Internet of Things，IoT）技术，用户设备（User Equipment，UE，也称为终端）或者无线接入网（Radio Access Network，RAN）可以作为读写器（Reader）来传输标签（tag）的数据。

射频识别（Radio Frequency Identification，RFID）技术中，读写器和标签（Tag）之间的信息传输工作在安全模式。对于工作在安全模式的标签，首先要执行鉴别（authentication，也可以译为鉴权）过程，具体而言，其通常包括读写器和/或标签的身份认证过程，从而在确定其身份合法的前提下，进行读写器和标签之间的信息传输。在RFID协议中，支持如下三种类型的鉴别/鉴权：

标签对读写器的单向鉴权，用于标签认证读写器是否通过鉴权，即读写器的身份是否合法；

读写器对标签的单向鉴权，用于读写器认证标签是否通过鉴权，即标签的身份是否合法；

双向鉴权，用于标签认证读写器是否通过鉴权和读写器认证标签是否通过鉴权，即读写器的身份是否合法，且标签的身份是否合法。

但是上述RFID技术中的鉴别/鉴权方案不能完全应用于3GPP相关的通信系统，其主要原因在于：RFID技术方案中是由读写器直接认证标签身份的合法性，但是迁移到3GPP相关的通信系统后，读写器可能是基于UE或者RAN实现，然而在3GPP系统中UE或者RAN自身也是一个不可信的节点。

因此，在3GPP相关的通信系统中，如何认证标签，以及，标签如何认证作为读写器的UE或者RAN，是亟待解决的问题。

发明内容

本申请实施例提供一种鉴权方法、鉴权装置、通信设备及可读存储介质，能够解决在3GPP系统中如何认证标签以及标签如何认证作为读写器的UE或者RAN的问题。

第一方面，提供了一种标签设备的鉴权方法，该方法包括：

第一设备发送第一鉴权命令，所述第一鉴权命令用于标签设备的认证，所述第一鉴权命令中包括所述标签设备的安全参数的配置信息；其中，所述第一设备为接入网设备、终端或核心网设备；

所述第一设备接收第一响应，所述第一响应中包括：所述标签设备的第一认证信息；

所述第一设备根据所述安全参数的配置信息和所述标签设备的第一认证信息，确定所述标签设备是否通过认证。

第二方面，提供了一种标签设备的鉴权方法，该方法包括：

标签设备接收第一设备发送的第一鉴权命令，所述第一鉴权命令用于所述标签设备的认证，所述第一鉴权命令中包括所述标签设备的安全参数的配置信息；所述第一设备为接入网设备、终端或核心网设备；

所述标签设备根据所述第一鉴权命令，向所述第一设备发送第一响应，所述第一响应中包括所述标签设备的第一认证信息。

第三方面，提供了一种读写器设备的鉴权方法，包括：

第一设备发送第二鉴权命令，所述第二鉴权命令用于读写器设备的认证，所述第二鉴权命令中包括标签设备的安全参数的配置信息和所述读写器设备的第三认证信息；其中，所述第一设备为所述读写器设备或核心网设备，所述读写器设备为接入网设备或终端；

所述第一设备接收第二响应，所述第二响应中包括：所述读写器设备通过认证或者未通过认证的鉴权结果。

第四方面，提供了一种读写器设备的鉴权方法，包括：

标签设备接收第一设备发送的第二鉴权命令，所述第二鉴权命令用于读写器设备的认证，所述第二鉴权命令中包括所述标签设备的安全参数的配置信息和所述读写器设备的第三认证信息；其中，所述第一设备为所述读写器设备或核心网设备，所述读写器设备为接入网设备或终端；

所述标签设备根据所述第二鉴权命令，确定所述读写器设备是否通过认证。

第五方面，提供了一种安全鉴权方法，该方法包括：

核心网设备接收读写器设备发送的请求，所述请求中包括标签设备的标识信息和/或用于计算所述读写器设备的认证信息的第二输入参数；所述读写器设备为接入网设备或终端；

所述核心网设备在向所述读写器设备发送所述标签设备的安全参数和/或所述读写器设备的第三认证信息，其中，所述第三认证信息由所述核心网设备根据所述标签设备的安全参数和所述第二输入参数通过计算确定。

第六方面，提供了一种标签设备的鉴权装置，包括：

第一发送模块，用于发送第一鉴权命令，所述第一鉴权命令用于标签设备的认证，所述第一鉴权命令中包括所述标签设备的安全参数的配置信息；其中，所述标签设备的鉴权装置为接入网设备、终端或核心网设备；

第一接收模块，用于接收第一响应，所述第一响应中包括：所述标签设备的第一认证信息；

第一确定模块，用于根据所述安全参数的配置信息和所述标签设备的第一认证信息，确定所述标签设备是否通过认证。

第七方面，提供了一种标签设备的鉴权装置，包括：

第一接收模块，用于接收第一设备发送的第一鉴权命令，所述第一鉴权命令用于所述标签设备的认证，所述第一鉴权命令中包括所述标签设备的安全参数的配置信息；所述第一设备为接入网设备、终端或核心网设备；

第一发送模块，用于根据所述第一鉴权命令，向所述第一设备发送第一响应，所述第一响应中包括所述标签设备的第一认证信息。

第八方面，提供了一种读写器设备的鉴权装置，包括：

第一发送模块，用于发送第二鉴权命令，所述第二鉴权命令用于读写器设备的认证，所述第二鉴权命令中包括标签设备的安全参数的配置信息和所述读写器设备的第三认证信息；其中，所述读写器设备的鉴权装置为所述读写器设备或核心网设备，所述读写器设备为接入网设备或终端；

第一接收模块，用于接收第二响应，所述第二响应中包括：所述读写器设备通过认证或者未通过认证的鉴权结果。

第九方面，提供了一种读写器设备的鉴权装置，包括：

第一接收模块，用于接收第一设备发送的第二鉴权命令，所述第二鉴权命令用于读写器设备的认证，所述第二鉴权命令中包括所述标签设备的安全参数的配置信息和所述读写器设备的第三认证信息；其中，所述第一设备为所述读写器设备或核心网设备，所述读写器设备为接入网设备或终端；

第一确定模块，用于根据所述第二鉴权命令，确定所述读写器设备是否通过认证。

第十方面，提供了一种安全鉴权装置，包括：

第一接收模块，用于接收读写器设备发送的请求，所述请求中包括标签设备的标识信息和/或用于计算所述读写器设备的认证信息的第二输入参数；所述读写器设备为接入网设备或终端；

第一发送模块，用于在向所述读写器设备发送所述标签设备的安全参数和/或所述读写器设备的第三认证信息，其中，所述第三认证信息由所述核心网设备根据所述标签设备的安全参数和所述第二输入参数通过计算确定。

第十一方面，提供了一种通信设备，该终端包括处理器和存储器，所述存储器存储可

在所述处理器上运行的程序或指令，所述程序或指令被所述处理器执行时实现如第一方面、第二方面、第三方面、第四方面或第五方面所述的方法的步骤。

第十二方面，提供了一种第一设备，包括处理器及通信接口，其中，所述通信接口用于发送第一鉴权命令，所述第一鉴权命令用于标签设备的认证，所述第一鉴权命令中包括所述标签设备的安全参数的配置信息；其中，所述第一设备为接入网设备、终端或核心网设备；接收第一响应，所述第一响应中包括：所述标签设备的第一认证信息；所述处理器用于根据所述安全参数的配置信息和所述标签设备的第一认证信息，确定所述标签设备是否通过认证。

第十三方面，提供了一种标签设备，包括处理器及通信接口，其中，所述通信接口用于接收第一设备发送的第一鉴权命令，所述第一鉴权命令用于所述标签设备的认证，所述第一鉴权命令中包括所述标签设备的安全参数的配置信息；所述第一设备为接入网设备、终端或核心网设备；根据所述第一鉴权命令，向所述第一设备发送第一响应，所述第一响应中包括所述标签设备的第一认证信息。

第十四方面，提供了一种第一设备，包括处理器及通信接口，其中，所述通信接口用于发送第二鉴权命令，所述第二鉴权命令用于读写器设备的认证，所述第二鉴权命令中包括标签设备的安全参数的配置信息和所述读写器设备的第三认证信息；其中，所述第一设备为所述读写器设备或核心网设备，所述读写器设备为接入网设备或终端；接收第二响应，所述第二响应中包括：所述读写器设备通过认证或者未通过认证的鉴权结果。

第十五方面，提供了一种标签设备，包括处理器及通信接口，其中，所述通信接口用于接收读写器设备发送的请求，所述请求中包括标签设备的标识信息和/或用于计算所述读写器设备的认证信息的第二输入参数；所述读写器设备为接入网设备或终端；所述处理器用于向所述读写器设备发送所述标签设备的安全参数和/或所述读写器设备的第三认证信息，其中，所述第三认证信息由所述核心网设备根据所述标签设备的安全参数和所述第二输入参数通过计算确定。

第十六方面，提供了一种核心网设备，包括处理器及通信接口，其中，所述通信接口用于接收第一设备发送的用于获取安全参数的第一请求，所述第一请求中包括标签设备的标识信息；所述第一设备为读写器设备，所述读写器设备为接入网设备或终端；在确定所述第一设备为可信设备的情况下，向所述第一设备发送所述标签设备的安全参数。

第十七方面，提供了一种可读存储介质，所述可读存储介质上存储程序或指令，所述程序或指令被处理器执行时实现如第一方面、第二方面、第三方面、第四方面或第五方面所述的方法的步骤。

第十八方面，提供了一种无线通信系统，包括：第一设备和标签设备，所述第一设备可用于执行如第一方面所述的方法的步骤，所述标签设备可用于执行如第二方面所述的方法的步骤，或者，所述第一设备可用于执行如第三方面所述的方法的步骤，所述标签设备可用于执行如第四方面所述的方法的步骤。

第十九方面，提供了一种无线通信系统，包括：第一设备、标签设备和核心网设备，所述第一设备可用于执行如第一方面所述的方法的步骤，所述标签设备可用于执行如第二方面所述的方法的步骤，所述核心网设备可用于执行如第五方面所述的方法的步骤。

第二十方面，提供了一种无线通信系统，包括：第一设备、标签设备和核心网设备，所述第一设备可用于执行如第三方面所述的方法的步骤，所述标签设备可用于执行如第四方面所述的方法的步骤，所述核心网设备可用于执行如第五方面所述的方法的步骤。

第二十一方面，提供了一种芯片，所述芯片包括处理器和通信接口，所述通信接口和所述处理器耦合，所述处理器用于运行程序或指令，实现如第一方面、第二方面、第三方面、第四方面或第五方面所述的方法。

第二十二方面，提供了一种计算机程序/程序产品，所述计算机程序/程序产品被存储在存储介质中，所述程序/程序产品被至少一个处理器执行以实现如第一方面、第二方面、第三方面、第四方面或第五方面所述的方法的步骤。

在本申请实施例中，明确了在无线通信系统中如何认证标签设备的流程，以及，标签设备如何认证作为读写器设备的 UE 或 RAN 的流程，以使得读写器设备和标签设备之间的信息传输工作在安全模式。

附图说明

图 1 为本申请实施例可应用的一种无线通信系统的框图；

图 2 为 UE 作为读写器（Reader）来传输 Ambient IoT（Tag）的数据到 Ambient IoT App 的示意图；

图 3 为 RAN 作为读写器（Reader）传输 Ambient IoT（Tag）的数据到 Ambient IoT App 的示意图；

图 4 为本申请实施例的标签设备的鉴权方法的流程示意图之一；

图 5 为本申请实施例的标签设备的鉴权方法的流程示意图之二；

图 6 为本申请实施例的读写器设备的鉴权方法的流程示意图之一；

图 7 为本申请实施例的读写器设备的鉴权方法的流程示意图之二；

图 8 为本申请实施例的安全鉴权方法的流程示意图；

图 9 为本申请实施例一的标签设备的鉴权方法的流程示意图；

图 10 为本申请实施例二的标签设备的鉴权方法的流程示意图；

图 11 为本申请实施例三的读写器设备的鉴权方法的流程示意图；

图 12 为本申请实施例四的读写器设备的鉴权方法的流程示意图；

图 13 为本申请实施例五的双向鉴权的方法的流程示意图；

图 14 为本申请实施例六的双向鉴权的方法的流程示意图；

图 15 为本申请实施例七的标签设备的鉴权方法的流程示意图；

图 16 为本申请实施例八的读写器设备的鉴权方法的流程示意图；

图 17 为本申请实施例九的双向鉴权的方法的流程示意图；

图 18 为本申请实施例的标签设备的鉴权装置的结构示意图之一；

图 19 为本申请实施例的标签设备的鉴权装置的结构示意图之二；

图 20 为本申请实施例的读写器设备的鉴权装置的结构示意图之一；

图 21 为本申请实施例的读写器设备的鉴权装置的结构示意图之二；

图 22 为本申请实施例的安全鉴权装置的结构示意图；

图 23 为本申请实施例的通信设备的结构示意图；

图 24 为本申请实施例的终端的硬件结构示意图；

图 25 为本申请实施例的网络侧设备的硬件结构示意图之一；

图 26 为本申请实施例的网络侧设备的硬件结构示意图之二。

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清楚描述，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所获得的所有其他实施例，都属于本申请保护的范围。

本申请的术语“第一”、“第二”等是用于区别类似的对象，而不用于描述特定的顺序或先后次序。应该理解这样使用的术语在适当情况下可以互换，以便本申请的实施例能够以除了在这里图示或描述的那些以外的顺序实施，且“第一”、“第二”所区别的对象通常为一类，并不限定对象的个数，例如第一对象可以是一个，也可以是多个。此外，本申请中的“或”表示所连接对象的至少其中之一。例如“A 或 B”涵盖三种方案，即，方案一：包括 A 且不包括 B；方案二：包括 B 且不包括 A；方案三：既包括 A 又包括 B。字符“/”一般表示前后关联对象是一种“或”的关系。

本申请的术语“指示”既可以是一个直接的指示（或者说显式的指示），也可以是一个间接的指示（或者说隐含的指示）。其中，直接的指示可以理解为，发送方在发送的指示中明确告知了接收方具体的信息、需要执行的操作或请求结果等内容；间接的指示可以理解为，接收方根据发送方发送的指示确定对应的信息，或者进行判断并根据判断结果确定需要执行的操作或请求结果等。

值得指出的是，本申请实施例所描述的技术不限于长期演进型（Long Term Evolution，LTE）/LTE 的演进（LTE-Advanced，LTE-A）系统，还可用于其他无线通信系统，诸如码分多址（Code Division Multiple Access，CDMA）、时分多址（Time Division Multiple Access，TDMA）、频分多址（Frequency Division Multiple Access，FDMA）、正交频分多址（Orthogonal Frequency Division Multiple Access，OFDMA）、单载波频分多址（Single-carrier Frequency-Division Multiple Access，SC-FDMA）或其他系统。本申请实施例中的术语“系统”和“网络”常被可互换地使用，所描述的技术既可用于以上提及的系统和无线电技术，也可用于其他系统和无线电技术。以下描述出于示例目的描述了新空口（New Radio，NR）系统，

并且在以下大部分描述中使用 NR 术语，但是这些技术也可应用于 NR 系统以外的系统，如第 6 代（6th Generation，6G）通信系统。

图 1 示出本申请实施例可应用的一种无线通信系统的框图。无线通信系统包括终端 11 和网络侧设备 12。其中，终端 11 可以是手机、平板电脑（Tablet Personal Computer）、膝上型电脑（Laptop Computer）、笔记本电脑、个人数字助理（Personal Digital Assistant，PDA）、掌上电脑、上网本、超级移动个人计算机（Ultra-mobile Personal Computer，UMPC）、移动上网装置（Mobile Internet Device，MID）、增强现实（Augmented Reality，AR）、虚拟现实（Virtual Reality，VR）设备、机器人、可穿戴式设备（Wearable Device）、飞行器（flight vehicle）、车载设备（Vehicle User Equipment，VUE）、船载设备、行人终端（Pedestrian User Equipment，PUE）、智能家居（具有无线通信功能的家居设备，如冰箱、电视、洗衣机或者家具等）、游戏机、个人计算机（Personal Computer，PC）、柜员机或者自助机等终端侧设备。可穿戴式设备包括：智能手表、智能手环、智能耳机、智能眼镜、智能首饰（智能手镯、智能手链、智能戒指、智能项链、智能脚镯、智能脚链等）、智能腕带、智能服装等。其中，车载设备也可以称为车载终端、车载控制器、车载模块、车载部件、车载芯片或车载单元等。需要说明的是，在本申请实施例并不限定终端 11 的具体类型。网络侧设备 12 可以包括接入网设备或核心网设备，其中，接入网设备也可以称为无线接入网（Radio Access Network，RAN）设备、无线接入网功能或无线接入网单元。接入网设备可以包括基站、无线局域网（Wireless Local Area Network，WLAN）接入点（Access Point，AS）或无线保真（Wireless Fidelity，WiFi）节点等。其中，基站可被称为节点 B（Node B，NB）、演进节点 B（Evolved Node B，eNB）、下一代节点 B（the next generation Node B，gNB）、新空口节点 B（New Radio Node B，NR Node B）、接入点、中继站（Relay Base Station，RBS）、服务基站（Serving Base Station，SBS）、基收发机站（Base Transceiver Station，BTS）、无线电基站、无线电收发机、基本服务集（Basic Service Set，BSS）、扩展服务集（Extended Service Set，ESS）、家用 B 节点（home Node B，HNB）、家用演进型 B 节点（home evolved Node B）、发送接收点（Transmission Reception Point，TRP）或所属领域中其他某个合适的术语，只要达到相同的技术效果，所述基站不限于特定技术词汇，需要说明的是，在本申请实施例中仅以 NR 系统中的基站为例进行介绍，并不限定基站的具体类型。

核心网设备可以包含核心网设备可以包含但不限于如下至少一项：核心网节点、核心网功能、移动管理实体（Mobility Management Entity，MME）、接入移动管理功能（Access and Mobility Management Function，AMF）、会话管理功能（Session Management Function，SMF）、用户平面功能（User Plane Function，UPF）、策略控制功能（Policy Control Function，PCF）、策略与计费规则功能单元（Policy and Charging Rules Function，PCRF）、边缘应用服务发现功能（Edge Application Server Discovery Function，EASDF）、统一数据管理（Unified Data Management，UDM）、统一数据仓储（Unified Data Repository，UDR）、归属用户服务器（Home Subscriber Server，HSS）、集中式网络配置（Centralized network configuration，

CNC）、网络存储功能（Network Repository Function，NRF）、网络开放功能（Network Exposure Function，NEF）、本地 NEF（Local NEF，或 L-NEF）、绑定支持功能（Binding Support Function，BSF）、应用功能（Application Function，AF）等。需要说明的是，在本申请实施例中仅以 NR 系统中的核心网设备为例进行介绍，并不限定核心网设备的具体类型。但不限于如下至少一项：核心网节点、核心网功能、移动管理实体（Mobility Management Entity，MME）、接入移动管理功能（Access and Mobility Management Function，AMF）、会话管理功能（Session Management Function，SMF）、用户平面功能（User Plane Function，UPF）、策略控制功能（Policy Control Function，PCF）、策略与计费规则功能单元（Policy and Charging Rules Function，PCRF）、边缘应用服务发现功能（Edge Application Server Discovery Function，EASDF）、统一数据管理（Unified Data Management，UDM）、统一数据仓储（Unified Data Repository，UDR）、归属用户服务器（Home Subscriber Server，HSS）、集中式网络配置（Centralized network configuration，CNC）、网络存储功能（Network Repository Function，NRF）、网络开放功能（Network Exposure Function，NEF）、本地 NEF（Local NEF，或 L-NEF）、绑定支持功能（Binding Support Function，BSF）、应用功能（Application Function，AF）等。需要说明的是，在本申请实施例中仅以 NR 系统中的核心网设备为例进行介绍，并不限定核心网设备的具体类型。

下面首先对本申请涉及的技术内容进行简单说明。

1、Ambient IoT

Ambient IoT（可以简称为 A-IOT）是一种待研究的新的 3GPP IoT 技术。Ambient IoT 设备具有超低复杂度以及超低的功耗。

Ambient IoT，又称为环境能量使能的物联网（Ambient power-enabled Internet of Things，Ambient power-enabled IoT），是一种 IoT 业务，其中 Ambient IoT 设备通过能量采集（energy harvesting）供能，Ambient IoT 设备没有电池，或者有有限的能量存储能力（例如，使用一个电容）。能量采集的能量源包括无线电波，光，运动，热或者其他合适的能量源。

Ambient IoT 设备的能量来自于能量采集。关于能量存储，Ambient IoT 设备可以具备以下特征：

1）无电池，无能量存储，完全依赖外部的能量源。或者，

2）有限的能量存储能力，无需换电池或充电。

Ambient IoT 设备可以基于能量源（energy source）、能量存储能力（energy storage capability）、被动（Passive）或主动（Active）发射等进行分类。

Ambient IoT 的被动（Passive）或主动（Active）发射，有如下多种通信模式：

1）正常操作。其中，Ambient IoT 设备有电能连续工作或持续工作一段时间。能量可以来自连续的能量采集，或可能具备有一定的能量储存能力，例如装配有电容。

2）主动发射，支持设备触发的操作。其中，设备仅能支持短时间的活动状态，支持间歇式通信。设备可以决定何时与网络通信。设备不一定监听网络，也就是可能长时间不监听被叫业务。

3）被动发射，仅支持网络发起的按需操作。其中，设备不能自己发起业务。

在3GPP系统中，Ambient IoT设备可以通过作为读写器（Reader）的UE或RAN，与Ambient IoT APP通信，参见图2和图3。其中，图2中，UE可以作为读写器（Reader）来传输Ambient IoT（Tag）的数据到 Ambient IoT App。图3中，RAN直接作为读写器（Reader）传输Ambient IoT（Tag）的数据到 Ambient IoT App。其中，5G核心网（5G core network，5GC）的参与是可选的。

2、反向散射通信（Backscatter Communication，BSC）

反向散射通信是指反向散射通信设备利用其它设备或者环境中的射频信号进行信号调制来传输自己信息。反向散射通信终端设备（BSC Tag，也可以称为BSC UE），可以是传统视频识别（Radio Frequency Identification，RFID）中的Tag，或环境储能的IoT（Ambient IoT），或者是无源IoT（Passive-IoT）设备。反向散射技术作为一种无源或者低耗能技术，其技术特点在于可以通过改变接收到的环境射频信号的特性例如相位或幅度信息来完成自身信号的传输，实现极低功耗或零功耗的信息传送。

3、RFID协议中读写器和标签之间的安全鉴别协议

RFID是一种传统的反向散射通信系统，其主要设计目标就是对读写器覆盖范围内的反向散射通信（BSC）设备（即Tag）进行标识（Identity document，ID）识别以及数据读取。

可选地，读写器和标签（Tag）之间的信息传输工作在安全模式。对于工作在安全模式的标签，首先要执行鉴别（authentication，也可以译为鉴权）过程，具体而言，其通常包括读写器和/或标签的身份认证过程，从而在确定其身份合法的前提下，进行读写器和标签之间的信息传输。在RFID协议中，支持如下三种类型的鉴别/鉴权：

标签对读写器的单向鉴权，用于标签认证读写器是否通过鉴权，即读写器的身份是否合法；

读写器对标签的单向鉴权，用于读写器认证标签是否通过鉴权，即标签的身份是否合法；

双向鉴权，用于标签认证读写器是否通过鉴权和读写器认证标签是否通过鉴权，即读写器的身份是否合法，且标签的身份是否合法。

目前协议仅标准化了标签的安全鉴权命令（Authenticate command）。对于安全鉴权协议流程具体需要几个步骤，支持的鉴权算法和流程等并未标准化。

下面结合附图，通过一些实施例及其应用场景对本申请实施例提供的鉴权方法、鉴权装置、通信设备及可读存储介质进行详细地说明。

请参考图4，本申请实施例提供一种标签设备的鉴权方法，包括：

步骤 41：第一设备发送第一鉴权命令，所述第一鉴权命令用于标签设备的认证，所述第一鉴权命令中包括所述标签设备的安全参数的配置信息；其中，所述第一设备为接入网（RAN）设备、终端（UE）或核心网设备；

可选的，所述核心网设备可以是相关技术中的核心网节点，如 AMF 等，也可以是新引入的核心网节点。

步骤 42：所述第一设备接收第一响应，所述第一响应中包括：所述标签设备的第一认证信息；

可选的，所述第一认证信息可以是认证码或数据签名。

步骤 43：所述第一设备根据所述安全参数的配置信息和所述标签设备的第一认证信息，确定所述标签设备是否通过认证。

在本申请实施例中，明确了在无线通信系统中如何认证标签设备的流程，以使得读写器设备（终端或接入网设备）和标签设备之间的信息传输工作在安全模式。

可选的，所述标签设备的安全参数（security credential）包括以下至少一项：根密钥（Root key，RK）索引（通过索引值唯一确定根密钥）、通信加密算法（用于指示标签设备支持的数据传输加密和完整性保护算法）、密钥长度、安全模式（用于指示标签设备是否需要进行安全鉴权，安全鉴权包括进行单向鉴权还是双向鉴权，单向鉴权是标签设备鉴权读写器设备还是读写器设备鉴权标签设备、是否需要进行安全通信）、安全功能（用于指示标签设备支持的安全鉴权算法，安全鉴权算法包括单向鉴权算法还是双向鉴权算法，单向鉴权算法是标签设备鉴权读写器设备使用的算法还是读写器设备鉴权标签设备使用的算法）、Tsec（读写器设备发送安全鉴权命令或安全通信命令后，等待标签设备响应的参考时间，以 10ms 为单位）。可选的，上述安全参数与标签设备的出产配置保持一致，写入标签设备后不可修改。

RFID 技术方案中，安全鉴权流程的前提步骤是，读写器需要触发安全参数获取流程，从标签获取标签的安全参数。但是迁移到 3GPP 系统后，读写器可能是基于接入网设备或终端实现，由于接入网设备或终端可能是不可信的节点，因此可以省略读写器从标签处获取标签的安全参数的流程。

本申请实施例中，可选的，当所述第一设备为接入网设备或终端时，可以考虑将所述标签设备的安全参数存储于所述第一设备中，可选的，运营商预先通过操作管理维护（Operation Administration Maintenance，OAM）的方式给所有可信的第一设备预配置该运营商管控的全部或部分标签设备的安全参数。

或者，考虑核心网设备作为一个可信的安全参数存储节点，所述安全参数由所述第一设备从核心网设备获取。此时，核心网设备可以对第一设备进行认证，如果认证第一设备是一个可信的节点，可以将标签设备的安全参数发送给第一设备，从而保证参与鉴权的接入网设备或终端是可信的设备。

本申请实施例中，可选的，所述第一设备为接入网设备或终端时，若第一设备支持存

储安全参数，在对标签设备进行鉴权之前，首先判断是否存有该标签设备的安全参数。

所述第一设备发送第一鉴权命令，包括：在所述第一设备有所述标签设备的安全参数的情况下，所述第一设备无需从核心网设备获取所述标签设备的安全参数，向标签设备发送第一鉴权命令。也就是说，在所述第一设备有所述标签设备的安全参数的情况下，第一设备可以直接向标签设备发送第一鉴权命令。

在所述第一设备没有所述标签设备的安全参数的情况下，所述第一设备发送第一鉴权命令之前，还包括：所述第一设备向核心网设备发送用于获取安全参数的第一请求，其中，所述第一请求中包括所述标签设备的标识信息；所述第一设备接收来自所述核心网设备的所述安全参数。也就是说，在所述第一设备没有所述标签设备的安全参数的情况下，第一设备先通过发送第一请求，请求获取安全参数，在获取到第一安全参数后，再向标签设备发送第一鉴权命令。

本实施例中，可选是第一设备支持预配置标签设备的安全参数的情况，当判断出有预配置的标签设备的安全参数时，则向标签设备发送第一鉴权命令，当判断出预配置标签设备的安全参数，则向核心网设备获取安全参数。

本申请实施例中，可选的，所述第一设备为接入网设备或终端；若第一设备不支持存储安全参数，在对标签设备进行鉴权之前，不需要判断是否存有该标签设备的安全参数。

此时，所述第一设备发送第一鉴权命令之前，还包括：

所述第一设备向核心网设备发送用于获取安全参数的第一请求，所述第一请求中包括所述标签设备的标识信息，其中，所述第一请求中包括所述标签设备的标识信息；

所述第一设备接收来自所述核心网设备的所述安全参数。

本实施例中，可以是第一设备不支持预配置标签设备的安全参数的情况，直接向核心网设备获取安全参数。

其中，可选的，所述标签设备的标识信息包括以下至少一项：所述标签设备的电子产品代码（Electronic Product code，EPC），所述标签设备的标签分配标识符（Tag identity，TID，该标签分配标识符存储在标签信息区中。标签信息区的数据在标签芯片出产时写入，写入后不能修改）。可选的，所述标签设备的标识信息与所述标签设备的出产配置保持一致，写入后不可修改。

本申请实施例中，可选的，所述第一设备为核心网设备；

所述第一设备发送第一鉴权命令包括：所述第一设备通过接入网设备向所述标签设备发送所述第一鉴权命令；

所述第一设备接收第一响应包括：所述第一设备接收接入网设备转发的所述第一响应；

本实施例中，接入网设备可以是透明转发所述第一鉴权命令和所述第一响应。

本申请实施例中，可选的，所述第一设备为所述标签设备的源服务小区所在的接入网设备；

所述第一设备发送第一鉴权命令包括：所述第一设备通过所述标签设备的目的服务小

区所在的接入网设备向所述标签设备发送所述第一鉴权命令，其中，所述标签设备的目的服务小区所在的接入网设备转发所述第一鉴权命令；

所述第一设备接收第一响应包括：所述第一设备接收所述标签设备的目的服务小区所在的接入网设备转发的所述第一响应。

本实施例中，所述标签设备的目的服务小区所在的接入网设备可以是透明转发所述第一鉴权命令和所述第一响应。

进一步地，标签设备的源服务小区所在的接入网设备可以给标签设备的目标服务小区所在的接入网设备通知标签设备是否通过认证的鉴权结果。这里的通知可以是显示的指示，也可以是隐式的指示，隐式方式例如通过目标服务小区所在的接入网设备发起与源服务小区所在的接入网设备之间的 UE 上下文获取流程实现，当标签设备的上下文获取成功，则认为标签设备通过认证；当标签设备上下文获取失败，则认为认证失败。

本申请实施例中，可选的，所述第一设备根据所述安全参数的配置信息和所述标签设备的第一认证信息，确定所述标签设备是否通过认证，包括：

所述第一设备根据所述标签设备的安全参数的配置信息和用于计算所述标签设备的第一认证信息的第一输入参数，通过计算确定所述标签设备的第二认证信息；

所述第一设备比较所述第二认证信息和接收到的所述标签设备的第一认证信息是否相同；

若所述第二认证信息和所述第一认证信息相同，确定所述标签设备通过认证；

若所述第二认证信息和所述第一认证信息不同，确定所述标签设备未通过认证。

本申请实施例中，不对第一认证信息和第二认证信息的计算方法进行限定，但是第一认证信息和第二认证信息的计算方法需要相同。

可选的，所述第一输入参数包括以下至少一项：所述标签设备的标识信息，所述标签设备的服务小区的标识信息，所述标签设备的上下文标识，所述第一认证信息传输对应的时间信息，所述第一认证信息传输对应的频域资源信息，所述第一认证信息传输对应的波束信息。

本申请实施例中，可选的，当所述第一设备为核心网设备时，所述第一设备根据第一输入参数以及所述标签设备的安全参数的配置信息，通过计算确定所述标签设备的第一认证信息之前还包括：所述第一设备接收所述标签设备的服务小区所在的接入网设备发送的所述第一输入参数。

可选的，所述第一输入参数包括以下至少一项：所述标签设备的标识信息，所述标签设备的服务小区的标识信息，所述标签设备的上下文标识，所述第一认证信息传输对应的时间信息，所述第一认证信息传输对应的频域资源信息，所述第一认证信息传输对应的波束信息。

本申请实施例中，可选的，所述第一设备为接入网设备或者终端，所述确定所述标签设备是否通过认证之后还包括：

若所述标签设备通过认证，所述第一设备执行以下至少一项：

1）向所述标签设备发送控制命令；

可选的，所述控制命令包括以下至少一项：

激活（Activate）命令，用于激活标签设备；

去激活（Deactivate）命令，用于去激活标签设备；

盘点（Inventory）命令，用于盘点标签设备；

读（Read）命令，用于从标签设备读取数据；

写（Write）命令，用于向标签设备写入数据；

定位（Positioning）命令，用于定位标签设备；

控制（Control）命令，用于控制标签设备。

2）接收所述标签设备发送的数据；

3）处理所述标签设备发送的数据；

4）转发所述标签设备发送的数据。

本申请实施例中，可选的，转发数据的对象可以是一个相关技术中的核心网设备，例如用户面功能（User plane Function，UPF），或者，一个新引入的核心网设备，或者 A-IOT App server 等，在此不做限定。

本申请实施例中，可选的，所述第一设备为核心网设备，所述确定所述标签设备是否通过认证之后还包括以下至少一项：

1）所述第一设备向接入网设备或终端发送所述标签设备是否通过认证的鉴权结果；

该种情况是核心网设备显式的将鉴权结果发送给接入网设备或终端。

2）所述第一设备向接入网设备或终端发送所述标签设备的授权信息，所述授权信息在所述标签设备通过认证的情况下发送。

该种情况下，核心网设备在标签设备通过认证的前提下向接入网设备或终端发送所述标签设备的授权信息，授权信息隐式表示通过标签设备通过认证。

请参考图 5，本申请实施例还提供一种标签设备的鉴权方法，包括：

步骤 51：标签设备接收第一设备发送的第一鉴权命令，所述第一鉴权命令用于所述标签设备的认证，所述第一鉴权命令中包括所述标签设备的安全参数的配置信息；所述第一设备为接入网设备、终端或核心网设备；

步骤 52：所述标签设备根据所述第一鉴权命令，向所述第一设备发送第一响应，所述第一响应中包括所述标签设备的第一认证信息。

可选的，所述第一认证信息可以是认证码或数据签名。

在本申请实施例中，明确了在 3GPP 系统中如何认证标签设备的流程，，以使得读写器设备（接入网设备或终端）和标签设备之间的信息传输工作在安全模式。

可选的，所述标签设备的安全参数（security credential）包括以下至少一项：根密钥（Root key，RK）索引（通过索引值唯一确定根密钥）、通信加密算法（用于指示标签设备

支持的数据传输加密和完整性保护算法）、密钥长度、安全模式（用于指示标签设备是否需要进行安全鉴权，安全鉴权包括进行单向鉴权还是双向鉴权，单向鉴权是标签设备鉴权读写器设备还是读写器设备鉴权标签设备、是否需要进行安全通信）、安全功能（用于指示标签设备支持的安全鉴权算法，安全鉴权算法包括单向鉴权算法还是双向鉴权算法，单向鉴权算法是标签设备鉴权读写器设备使用的算法还是读写器设备鉴权标签设备使用的算法）、Tsec（读写器设备发送安全鉴权命令或安全通信命令后，等待标签设备响应的参考时间，以 10ms 为单位）。可选的，上述安全参数与标签设备的出产配置保持一致，写入标签设备后不可修改。

本申请实施例中，可选的，当所述第一设备为接入网设备或终端时，可以考虑将所述标签设备的安全参数存储于所述第一设备中，可选的，运营商预先通过操作管理维护（Operation Administration Maintenance，OAM）的方式给所有可信的第一设备预配置该运营商管控的全部或部分标签设备的安全参数。

或者，考虑核心网设备作为一个可信的安全参数存储节点，所述安全参数由所述第一设备从核心网设备获取。此时，核心网设备可以对第一设备进行认证，如果认证第一设备是一个可信的节点，可以将标签设备的安全参数发送给第一设备，从而保证参与鉴权的接入网设备或终端是可信的设备。

本申请实施例中，可选的，所述标签设备根据所述第一鉴权命令，向所述第一设备发送第一响应，包括：

所述标签设备根据所述安全参数的配置信息和用于计算所述标签设备的第一认证信息的第一输入参数，通过计算确定所述标签设备的第一认证信息；

所述标签设备向所述第一设备发送所述第一响应，所述第一响应中包括所述第一认证信息。

本申请实施例中，可选的，所述第一输入参数包括以下至少一项：所述标签设备的标识信息，所述标签设备的服务小区的标识信息，所述标签设备的上下文标识，所述第一认证信息传输对应的时间信息，所述第一认证信息传输对应的频域资源信息，所述第一认证信息传输对应的波束信息。

上述实施例是对标签设备的鉴权，下面介绍对读写器设备的鉴权。

请参考图 6，本申请实施例还提供一种读写器设备的鉴权方法，包括：

步骤 61：第一设备发送第二鉴权命令，所述第二鉴权命令用于读写器设备的认证，所述第二鉴权命令中包括标签设备的安全参数的配置信息和所述读写器设备的第三认证信息；其中，所述第一设备为所述读写器设备或核心网设备，所述读写器设备为接入网设备或终端；

可选的，所述第三认证信息可以是认证码或数据签名。

步骤 62：所述第一设备接收第二响应，所述第二响应中包括：所述读写器设备通过认证或者未通过认证的鉴权结果。

在本申请实施例中，明确了在 3GPP 系统中标签设备如何认证作为读写器设备的 UE 或 RAN 的流程，以使得读写器设备和标签设备之间的信息传输工作在安全模式。

本申请实施例中，可选的，当所述第一设备为接入网设备或终端时，可以考虑将所述标签设备的安全参数存储于所述第一设备中，可选的，运营商预先通过操作管理维护（Operation Administration Maintenance，OAM）的方式给所有可信的第一设备预配置该运营商管控的全部或部分标签设备的安全参数。

或者，考虑核心网设备作为一个可信的安全参数存储节点，所述安全参数由所述第一设备从核心网设备获取。此时，核心网设备可以对第一设备进行认证，如果认证第一设备是一个可信的节点，可以将标签设备的安全参数发送给第一设备，从而保证参与鉴权的接入网设备或终端是可信的设备。

本申请实施例中，可选的，所述第一设备发送第二鉴权命令之前还包括：所述第一设备确定所述读写器设备的第三认证信息。

本申请实施例中，可选的，所述第一设备为所述读写器设备，所述第一设备发送第二鉴权命令之前还包括：

所述第一设备向核心网设备发送用于获取安全参数的第一请求（该种情况通常是第一设备不支持预配置标签设备的安全参数的情况，则直接向核心网设备获取安全参数）；

或者，

在所述第一设备没有所述标签设备的安全参数的情况下，所述第一设备向核心网设备发送用于获取安全参数的第一请求（该种情况通常时第一设备支持预配置标签设备的安全参数的情况，如果没有判断没有预配置标签设备的安全参数，则向核心网设备获取安全参数）；

其中，所述第一请求中包括所述标签设备的标识信息。

本申请实施例中，可选的，所述第一设备为读写器设备，所述第一设备发送第二鉴权命令之前还包括：

所述第一设备向核心网设备发送用于获取安全参数的第一请求，所述第一请求中包括所述标签设备的标识信息和用于计算所述读写器设备的第三认证信息的第二输入参数（该种情况通常是第一设备不支持预配置标签设备的安全参数的情况，则直接向核心网设备获取安全参数，同时还需要请求核心网设备来计算读写器设备的第三认证信息）；

所述第一设备接收所述核心网设备发送的所述标签设备的安全参数和所述读写器设备的第三认证信息；

或者，

在所述第一设备有所述标签设备的安全参数的情况下，所述第一设备向核心网设备发送第二请求；所述第一设备接收所述核心网设备发送的所述读写器设备的第三认证信息（该种情况通常是第一设备支持预配置标签设备的安全参数的情况，如果判断有预配置标签设备的安全参数，则无需向核心网设备获取安全参数，只需要请求核心网设备来计算读

写器设备的第三认证信息即可）；

在所述第一设备没有所述标签设备的安全参数的情况下，所述第一设备向核心网设备发送用于获取安全参数的第一请求；所述第一设备接收所述核心网设备发送的所述标签设备的安全参数和所述读写器设备的第三认证信息（该种情况通常是第一设备支持预配置标签设备的安全参数的情况，如果判断没有预配置标签设备的安全参数，则向核心网设备获取安全参数，同时还需要请求核心网设备来计算读写器设备的第三认证信息）；

其中，所述第一请求中包括所述标签设备的标识信息和用于计算所述读写器设备的第三认证信息的第二输入参数，所述第二请求中包括用于计算所述读写器设备的第三认证信息的第二输入参数。

本申请实施例中，可选的，所述第二输入参数包括以下至少一项：所述第一设备的标识信息，所述第三认证信息传输对应的时间信息，所述第三认证信息传输对应的频域资源信息，所述第三认证信息传输对应的波束信息。

本申请实施例中，可选的，所述第一设备为核心网设备；

所述第一设备发送第二鉴权命令包括：所述第一设备向通过接入网设备向所述标签设备发送所述第二鉴权命令；

所述第一设备接收第二响应包括：所述第一设备接收由所述接入网设备转发的所述第二响应。

本实施例中，可选的，所述接入网设备可以透明转发所述第二鉴权命令和所述第二响应。

本申请实施例中，可选的，所述第一设备接收第二响应之后还包括：

所述第一设备发送第一鉴权命令，所述第一鉴权命令用于对标签设备进行认证，所述第一鉴权命令中包括所述标签设备的安全参数的配置信息；

所述第一设备接收第一响应，所述第一响应中包括：所述标签设备的第一认证信息；

所述第一设备根据所述安全参数的配置信息和所述标签设备的第一认证信息，确定所述标签设备是否通过认证。

本申请实施例中，标签设备先对读写器设备进行鉴权，然后再由读写器设备对标签设备进行鉴权。当然，在本申请的其他一些实施例中，也不排除，读写器设备先对标签设备进行鉴权，然后再由标签设备先对读写器设备进行鉴权。

请参考图 7，本申请实施例还提供一种读写器设备的鉴权方法，包括：

步骤 71：标签设备接收第一设备发送的第二鉴权命令，所述第二鉴权命令用于读写器设备的认证，所述第二鉴权命令中包括所述标签设备的安全参数的配置信息和所述读写器设备的第三认证信息；其中，所述第一设备为所述读写器设备或核心网设备，所述读写器设备为接入网设备或终端；

可选的，所述第三认证信息可以是认证码或数据签名。

步骤 72：所述标签设备根据所述第二鉴权命令，确定所述读写器设备是否通过认证。

在本申请实施例中，明确了在 3GPP 系统中标签设备如何认证作为读写器设备的 UE 或 RAN 的流程，以使得读写器设备和标签设备之间的信息传输工作在安全模式。

RFID 技术方案中，安全鉴权流程的前提步骤是，读写器需要触发安全参数获取流程，从标签获取标签的安全参数。但是迁移到 3GPP 系统后，读写器可能是基于接入网设备或终端实现，由于接入网设备或终端可能是不可信的节点，因此可以省略读写器从标签处获取标签的安全参数的流程。本申请实施例中，可选的，当所述第一设备为接入网设备或终端时，可以考虑将所述标签设备的安全参数存储于所述第一设备中，标签设备的安全参数存储于所述第一设备中，可以是，标签设备的安全参数通过预配置的方式预配置到所述第一设备中。或者，考虑核心网设备作为一个可信的安全参数存储节点，所述安全参数由所述第一设备从核心网设备获取。此时，核心网设备可以对第一设备进行认证，如果认证第一设备是一个可信的节点，可以将标签设备的安全参数发送给第一设备，从而保证参与鉴权的接入网设备或终端是可信的设备。

本申请实施例中，可选的，所述标签设备根据所述第二鉴权命令，确定所述读写器设备是否通过认证，包括：

所述标签设备根据所述标签设备的安全参数的配置信息和用于计算所述读写器设备的第三认证信息的第二输入参数，通过计算确定所述读写器设备的第四认证信息；

所述标签设备比较所述第四认证信息和接收到的所述读写器设备的第三认证信息是否相同；

若所述第四认证信息和所述第三认证信息相同，确定所述读写器设备通过认证；

若所述第四认证信息和所述第三认证信息不同，确定所述读写器设备未通过认证。

本申请实施例中，不对第三认证信息和第四认证信息的计算方法进行限定，但是第三认证信息和第四认证信息的计算方法需要相同。

本申请实施例中，可选的，所述第二输入参数包括以下至少一项：所述第一设备的标识信息，所述第三认证信息传输对应的时间信息，所述第三认证信息传输对应的频域资源信息，所述第三认证信息传输对应的波束信息。

本申请实施例中，可选的，所述标签设备根据所述第二鉴权命令，确定所述读写器设备是否通过认证之后还包括：

若所述读写器设备通过认证，所述标签设备执行以下至少一项：

向所述第一设备发送第二响应，所述第二响应中包括：所述读写器设备通过认证或者未通过认证的鉴权结果；

1）响应所述读写器设备发送的控制命令；

可选的，所述控制命令包括以下至少一项：

激活（Activate）命令，用于激活标签设备；

去激活（Deactivate）命令，用于去激活标签设备；

盘点（Inventory）命令，用于盘点标签设备；

读（Read）命令，用于从标签设备读取数据;

写（Write）命令，用于向标签设备写入数据;

定位（Positioning）命令，用于定位标签设备;

控制（Control）命令，用于控制标签设备。

2）向所述读写器设备发送数据。

本申请实施例中，可选的，所述标签设备接收第一设备发送的第二鉴权命令之后还包括:

所述标签设备接收所述第一设备发送的第一鉴权命令，所述第一鉴权命令用于对所述标签设备进行认证，所述第一鉴权命令中包括所述标签设备的安全参数的配置信息;

所述标签设备根据所述第一鉴权命令，确定所述标签设备的第一认证信息;

所述标签设备向所述第一设备发送第一响应，所述第一响应中包括：所述标签设备的第一认证信息。

本申请实施例中，标签设备先对读写器设备进行鉴权，然后再由读写器设备对标签设备进行鉴权。当然，在本申请的其他一些实施例中，也不排除，读写器设备先对标签设备进行鉴权，然后再由标签设备先对读写器设备进行鉴权。

本申请实施例中，可选的，所述标签设备根据所述第二鉴权命令，确定所述读写器设备是否通过认证之后还包括:

若所述读写器设备未通过认证，所述标签设备丢弃所述第一设备发送的第一鉴权命令，所述第一鉴权命令用于对所述标签设备进行认证，所述第一鉴权命令中包括所述标签设备的安全参数的配置信息。

本申请实施例中，标签设备先对读写器设备进行鉴权，然后再由读写器设备对标签设备进行鉴权，如果所述读写器设备未通过认证，则标签设备不再对读写器设备进行鉴权。

请参考图 8，本申请实施例还提供一种安全鉴权方法，包括:

步骤 81: 核心网设备接收读写器设备发送的请求，所述请求中包括标签设备的标识信息和/或用于计算所述读写器设备的认证信息的第二输入参数；所述读写器设备为接入网设备或终端;

步骤 82: 所述核心网设备向所述读写器设备发送所述标签设备的安全参数和/或所述读写器设备的第三认证信息，其中，所述第三认证信息由所述核心网设备根据所述标签设备的安全参数和所述第二输入参数通过计算确定。

本申请实施例中，作为读写器设备的接入网设备或终端在对标签设备进行鉴权之前，或者，请求标签设备对所述读写器设备进行鉴权之前，可以向核心网设备获取标签设备的安全参数和/或请求核心网设备确定读写器设备的认证信息，核心网设备验证读写器设备可信的情况下，再向读写器设备发送所述标签设备的安全参数和/或读写器设备的认证信息，从而保证参与鉴权的接入网设备或终端是可信的设备。

在一些实施例中，可选的，核心网设备接收读写器设备发送的请求，所述请求中包括

标签设备的标识信息，此时，核心网设备向所述读写器设备发送所述标签设备的安全参数。即读写器设备仅请求标签设备的安全参数。

在一些实施例中，可选的，核心网设备接收读写器设备发送的请求，所述请求中包括用于计算所述读写器设备的认证信息的第二输入参数，此时，核心网设备向所述读写器设备发送所述读写器设备的第三认证信息。即读写器设备仅请求请求核心网设备确定读写器设备的认证信息。

在一些实施例中，可选的，核心网设备接收读写器设备发送的请求，所述请求中包括标签设备的标识信息和用于计算所述读写器设备的认证信息的第二输入参数，此时，核心网设备向所述读写器设备发送所述标签设备的安全参数和所述读写器设备的第三认证信息。即读写器设备既请求标签设备的安全参数，又请求核心网设备确定读写器设备的认证信息。

本申请实施例中，可选的，所述核心网设备向所述读写器设备发送所述标签设备的安全参数和/或所述读写器设备的第三认证信息包括:

所述核心网设备在判断所述读写器设备可信的情况下，向所述读写器设备发送所述标签设备的安全参数和/或所述读写器设备的第三认证信息。

本申请实施例中，核心网设备可以用于为读写器设备计算认证信息。

下面结合具体应用场景，对本申请实施例的上述方法举例进行说明。

本申请实施例一

本实施例中，RAN 节点（接入网设备）作为读写器设备，A-IOT 设备作为标签设备，本实施例是 RAN 节点对 A-IOT 设备的单向鉴权，即 RAN 节点认证 A-IOT 设备是否合法，安全功能的对等实体为 A-IOT 设备和 RAN 节点。

请参考图 9，本申请实施例的标签设备的鉴权方法包括:

步骤 0a 和步骤 0b 为可选步骤，具体方式通过以下 1）或 2）任一项实现:

1) 运营商预先通过操作管理维护（Operation Administration Maintenance，OAM）方式给所有可信 RAN 节点预配置该运营商管控的全部或部分 A-IOT 设备的安全参数（security credential）。对于某个特定 RAN 节点，其在触发与 A-IOT 设备之间的空口安全鉴权流程之前，首先判断其预配置中是否存有该 A-IOT 设备的安全参数。

a. 若该 A-IOT 设备的安全参数在其预配置中，则可跳过步骤 0a 和步骤 0b，RAN 节点直接触发空口的安全鉴权流程，即 RAN 节点第一步执行图 9 中的步骤 1。

b. 若接入该 RAN 节点的 A-IOT 设备的安全参数不在其预配置中，则 RAN 节点在触发空口的安全鉴权流程之前，先向 5GC 节点请求该 A-IOT 设备的安全参数，请求中携带该 A-IOT 设备的标识（Identifier，ID）信息，5GC 节点在判断 RAN 节点可信的前提下，向 RAN 节点响应该 A-IOT 设备的安全参数。即 RAN 节点第一步执行步骤 0a 和步骤 0b。该 5GC 节点可以是相关技术的 5GC 节点(例如接入和移动性管理功能(Access and Mobility Management Function，AMF))，或者新引入的 5GC 功能节点，在此不做限定。

2) 运营商未支持通过OAM方式给所有可信RAN节点预配置该运营商管控的全部或部分A-IOT设备的安全参数（security credential）的情况下，对于某个特定RAN节点，在触发空口的安全鉴权流程之前，总是先向5GC节点请求该A-IOT设备的安全参数，5GC节点在判断RAN节点可信的前提下，向RAN节点响应该A-IOT设备的安全参数，即RAN节点第一步执行步骤0a，步骤0b是否执行取决于5GC节点判断RAN节点是否可信。

其中，A-IOT设备的ID信息，可以包括以下至少一项：A-IOT设备的电子产品代码（Electronic Product code，EPC），A-IOT设备的标签分配标识符（Tag identity，TID），该标签分配标识符存储在标签信息区中。标签信息区的数据在标签芯片出产时写入，写入后不能修改）。上述ID信息与A-IOT设备的出产配置保持一致，写入后不可修改。

所述 A-IOT 设备的安全参数可以包括以下至少一项：根密钥（Root key，RK）索引（通过索引值唯一确定根密钥）、通信加密算法（用于指示A-IOT设备支持的数据传输加密和完整性保护算法）、密钥长度、安全模式（用于指示A-IOT设备是否需要进行安全鉴权，安全鉴权包括进行单向鉴权还是双向鉴权，单向鉴权是A-IOT设备鉴权RAN节点还是RAN节点鉴权A-IOT设备、是否需要进行安全通信）、安全功能（用于指示A-IOT设备支持的安全鉴权算法，安全鉴权算法包括单向鉴权算法还是双向鉴权算法，单向鉴权算法是A-IOT设备鉴权RAN节点使用的算法还是RAN节点鉴权A-IOT设备使用的算法）、Tsec（RAN节点发送安全鉴权命令或安全通信命令后，等待A-IOT设备响应的参考时间，以10ms为单位）。上述安全参数与A-IOT设备的出产配置保持一致，写入A-IOT设备后不可修改。

步骤1：RAN节点向A-IOT设备发送单向鉴权命令（即上述实施例中的第一鉴权命令），所述单向鉴权命令用于A-IoT设备的鉴权，所述单向鉴权命令至少携带A-IOT设备的安全参数的配置信息，该配置信息遵循RAN节点的预配置的安全参数的内容或者遵循从5GC节点获取的安全参数的配置内容（即步骤0b）。

根据步骤1，A-IOT设备通过计算确定A-IOT设备的认证码或数据签名。其中A-IOT设备生成A-IOT设备认证码或数据签名的方法，本申请不作限定。

步骤2：A-IOT设备向RAN节点发送单向鉴权命令的响应（第一响应），所述单向鉴权命令的响应中携带：A-IOT设备的ID信息，A-IOT设备的认证码或数据签名。

根据步骤2，RAN节点确定A-IOT设备是否通过认证，具体的，可以根据以下方法确定：

该RAN节点通过确定A-IOT设备的认证码或数据签名，比对自己计算并生成的A-IOT设备的认证码或数据签名，与步骤2中收到的A-IOT设备的认证码或数据签名，如果两者取值相等，则判断A-IOT设备通过认证；否则，判断A-IOT设备认证失败。

本申请实施例中，可选的，若该RAN节点为所述A-IOT设备的源服务小区所在的RAN节点；A-IOT设备的源服务小区所在的RAN节点通过计算确定A-IOT设备的认证码或数据签名，比对自己计算并生成的A-IOT设备的认证码或数据签名，与步骤2中收到

的 A-IOT 设备的认证码或数据签名，如果两者取值相等，则判断 A-IOT 设备通过认证；否则，判断 A-IOT 设备认证失败。

进一步地，A-IOT 设备的源服务小区所在的 RAN 节点可以给 A-IOT 设备的目标服务小区所在的 RAN 节点通知 A-IOT 设备是否通过认证的鉴权结果。这里的通知可以是显示的指示，也可以是隐式的指示，隐式方式例如通过目标服务小区所在的 RAN 节点发起与源服务小区所在的 RAN 节点之间的 UE 上下文获取流程实现，当 A-IOT 设备的上下文获取成功，则认为 A-IOT 设备通过认证；当 A-IOT 设备上下文获取失败，则认为认证失败。

其中 A-IOT 设备的源服务小区所在的 RAN 节点计算并生成 A-IOT 设备的认证码或数据签名的方法，本申请不作限定。但须与 A-IOT 设备生成 A-IOT 设备的认证码或数据签名的方法，保持一致。

进一步地，在该 RAN 节点确定 A-IOT 设备通过认证的前提下，RAN 节点执行以下至少一项：

向 A-IOT 设备发送控制命令；

接收或处理 A-IOT 设备的数据；

转发 A-IOT 设备的数据。

这里，转发数据的对象可以是一个相关技术的 5GC 节点，例如用户面功能（User plane Function，UPF），或者，一个新引入的 5GC 功能节点，或者 A-IOT App server 等，在此不做限定。

本申请实施例二

本实施例中，RAN 节点（接入网设备）作为读写器设备，A-IOT 设备作为标签设备，本实施例是 5GC 节点（核心网设备）对 A-IOT 设备的单向鉴权，即 5GC 节点认证 A-IOT 设备是否合法，安全功能的对等实体为 A-IOT 设备和 5GC 节点。

实施例二与实施例一的区别自于： RAN 节点承担的是安全鉴权相关命令的透明转发功能，实质不参与 A-IOT 设备的安全鉴权功能，生成安全鉴权命令以及执行鉴权功能的是 5GC 节点。

请参考图 10，本申请实施例的标签设备的鉴权方法包括：

步骤 1：5GC 节点向 A-IOT 设备发送单向鉴权命令（即上述实施例中的第一鉴权命令），所述单向鉴权命令通过 RAN 节点透明转发至 A-IOT 设备。所述单向鉴权命令用于 A-IoT 设备的鉴权，所述单向鉴权命令至少携带 A-IOT 设备的安全参数的配置信息。

根据步骤 1，A-IOT 设备通过计算确定 A-IOT 设备的认证码或数据签名。其中 A-IOT 设备生成 A-IOT 设备的认证码或数据签名的方法，本申请不作限定。

步骤 2：A-IOT 设备向 5GC 节点发送单向鉴权命令的响应（第一响应），所述单向鉴权命令的响应通过 RAN 节点透明转发至 5GC 节点。所述单向鉴权命令的响应中携带：A-IOT 设备的 ID 信息，A-IOT 设备的认证码或数据签名。

步骤 3：RAN 节点转发单向鉴权命令的响应，还将用于计算 A-IOT 设备的认证码或

数据签名的至少一个第一输入参数发送给 5GC 节点。

根据步骤 3，5GC 节点确定 A-IOT 设备是否通过认证，可以通过以下方式确定：

该 5GC 节点通过计算确定 A-IOT 设备的认证码或数据签名，比对自己计算并生成 A-IOT 设备的认证码或数据签名，与收到的 A-IOT 设备的认证码或数据签名，如果两者取值相等，则判断 A-IOT 设备通过认证；否则，判断 A-IOT 设备认证失败；

其中 5GC 节点计算并生成 A-IOT 设备的认证码或数据签名的方法，本申请不作限定。但须与 A-IOT 设备生成 A-IOT 设备的认证码或数据签名的方法，保持一致。

步骤 4：5GC 节点向 RAN 节点反馈所述 A-IOT 设备是否通过认证的鉴权结果。

根据步骤 4，进一步地，在该 RAN 节点确定 A-IOT 设备通过认证的前提下，RAN 节点执行以下至少一项：

向 A-IOT 设备发送其他命令；

接收或处理 A-IOT 设备的数据；

转发 A-IOT 设备的数据。

这里，转发数据的对象可以是一个相关技术的 5GC 节点，例如用户面功能（User plane Function，UPF），或者，一个新引入的 5GC 功能节点，或者 A-IOT App server 等，在此不做限定。

本申请实施例三

本实施例中，RAN 节点（接入网设备）作为读写器设备，A-IOT 设备作为标签设备，本实施例是 A-IOT 设备对 RAN 节点的单向鉴权，即 A-IOT 设备认证 RAN 节点是否合法，安全功能的对等实体为 A-IOT 设备和 RAN 节点。

请参考图 11，本申请实施例的读写器设备的鉴权方法包括：

步骤 0a 和步骤 0b 描述同实施例一，不再重复描述。

步骤 1：RAN 节点向 A-IOT 设备发送请求单向鉴权命令（第二鉴权命令），所述请求单向鉴权命令用于 RAN 节点的鉴权，所述请求单向鉴权命令至少携带 A-IOT 设备的安全参数的配置信息，RAN 节点的认证码或数据签名。

在步骤 1 之前，RAN 节点通过计算确定 RAN 节点的认证码或数据签名。其中 RAN 节点生成 RAN 节点认证码或数据签名的方法，本申请不作限定。

步骤 2：A-IOT 设备向 RAN 节点发送请求单向鉴权命令的响应（即第二响应），所述请求单向鉴权命令的响应携带 RAN 节点是否通过认证的鉴权结果。

在步骤 2 之前，A-IOT 设备确定 RAN 节点是否通过认证。可选的，可以通过以下方法确定：该 A-IOT 设备自己计算并生成 RAN 节点的认证码或数据签名，比对自己计算并生成 RAN 节点的认证码或数据签名，与步骤 1 中收到的 RAN 节点的认证码或数据签名，如果两者取值相等，则判断 RAN 节点通过认证；否则，判断 RAN 节点认证失败。

其中 A-IOT 设备生成 RAN 节点认证码或数据签名的方法，本申请不作限定。但须与 RAN 节点生成 RAN 节点认证码或数据签名的方法，保持一致。

进一步地，在该 A-IOT 设备确定 RAN 节点通过认证的前提下，A-IOT 设备执行以下至少一项：

响应 RAN 节点发送的控制命令；

向 RAN 节点发送 A-IOT 设备的数据。

本申请实施例四

本实施例中，RAN 节点（接入网设备）作为读写器设备，A-IOT 设备作为标签设备，本实施例是 A-IOT 设备对 RAN 节点的单向鉴权，即 A-IOT 设备认证 RAN 节点是否合法，安全功能的对等实体为 A-IOT 设备和 5GC 节点（核心网设备）。

请参考图 12，本申请实施例的读写器设备的鉴权方法包括：

步骤 0a 和步骤 0b 为可选步骤，具体方式通过以下 1）或 2）任一项实现：

1）运营商预先通过操作管理维护（Operation Administration Maintenance，OAM）方式给所有可信 RAN 节点预配置该运营商管控的全部或部分 A-IOT 设备的安全参数（security credential）。对于某个特定 RAN 节点，其在触发与 A-IOT 设备之间的空口安全鉴权流程之前，首先判断其预配置中是否存有该 A-IOT 设备的安全参数。

a. 若该 A-IOT 设备的安全参数在其预配置中， 则在步骤 0a 中向 5GC 节点发送用于计算 RAN 节点的认证码或数字签名的部分或全部第二输入参数（如 A-IOT 设备 ID，A-IOT 设备的服务小区 ID、A-IOT 设备的 UE context ID，认证码或数据签名传输对应的时间信息、认证码或数据签名传输对应的频域资源信息、认证码或数据签名传输对应的波束信息中的至少一项），步骤 0b：5GC 节点向所述 RAN 节点返回所述 RAN 节点的认证码或数字签名。

b. 若该 A-IOT 设备的安全参数不在其预配置中，则在步骤 0a 中，向 5GC 节点发送获取该 A-IOT 设备的安全参数的请求，并携带 A-IOT 设备的 ID 信息和用于计算 RAN 节点的认证码或数字签名的部分或全部第二输入参数，步骤 0b：5GC 节点向所述 RAN 节点返回该 A-IOT 设备的安全参数和所述 RAN 节点的认证码或数字签名。

这里，5GC 节点可以是相关技术中的 5GC 节点（例如 AMF），或者新引入的 5GC 功能节点，在此不做限定。

也就是说，本实施例中，由 5GC 节点计算 RAN 节点的认证码或数字签名。

2）运营商未支持通过 OAM 方式给所有可信 RAN 节点预配置该运营商管控的全部或部分 A-IOT 设备的安全参数（security credential）的情况下，对于某个特定 RAN 节点，则 RAN 节点在触发空口的安全鉴权流程之前，总是先向 5GC 节点请求该 A-IOT 设备的安全参数，并发送用于计算 RAN 的认证码或数字签名的第二输入参数，5GC 节点在判断 RAN 节点可信的前提下，向 RAN 节点响应该 A-IOT 设备的安全参数和所述 RAN 的节点的认证码或数字签名。即 RAN 节点第一步执行步骤 0a，步骤 0b 是否执行取决于 5GC 节点判断 RAN 节点是否可信的认证结果。

步骤 1：RAN 节点向 A-IOT 设备发送请求单向鉴权命令（即上述实施例中的第二鉴

权命令），所述请求单向鉴权命令用于 RAN 节点的鉴权，所述请求单向鉴权命令至少携带 A-IOT 设备的安全参数的配置信息，RAN 节点的认证码或数据签名。该配置内容遵循 RAN 节点的预配置内容或者遵循 5GC 节点返回的配置内容（即步骤 0b）；

或者，也可以由 5GC 节点向 A-IOT 设备发送请求单向鉴权命令，所述请求单向鉴权命令通过 RAN 节点透明转发至 A-IOT 设备。

在步骤 1 之前，5GC 节点计算并生成 RAN 节点的认证码或数据签名。其中 5GC 节点生成 RAN 节点的认证码或数据签名的方法，本申请不作限定。

步骤 2：A-IOT 设备向 RAN 节点发送请求单向鉴权命令的响应（即第二响应），所述请求单向鉴权命令的响应至少携带 RAN 节点是否通过认证的鉴权结果。

或者，A-IOT 设备向 5GC 节点发送请求单向鉴权命令的响应，所述请求单向鉴权命令的响应通过 RAN 节点透明转发至 5GC 节点。

在步骤 2 之前，A-IOT 设备确定 RAN 节点是否通过认证。可选的，可以通过以下方法确定：该 A-IOT 设备自己计算并生成 RAN 节点的认证码或数据签名，比对自己计算并生成 RAN 节点的认证码或数据签名，与步骤 1 中收到的 RAN 节点的认证码或数据签名，如果两者取值相等，则判断 RAN 节点通过认证；否则，判断 RAN 节点认证失败。

其中 A-IOT 设备生成 RAN 节点认证码或数据签名，本申请不作限定。但须与 5GC 节点生成 RAN 节点认证码或数据签名的方法，保持一致。

进一步地，在该 A-IOT 设备确定 RAN 节点通过认证的前提下，A-IOT 设备执行以下至少一项：

响应 RAN 节点发送的其他命令；

向 RAN 节点发送 A-IOT 设备的数据。

本申请实施例五

本实施例中，RAN 节点（接入网设备）作为读写器设备，A-IOT 设备作为标签设备，本实施例是 A-IOT 设备和 RAN 节点的双向鉴权，即 A-IOT 设备认证 RAN 节点是否合法，且 RAN 节点认证 A-IOT 设备是否合法，安全功能的对等实体为 A-IOT 设备和 RAN 节点。

参见图 13，本申请实施例的方法可视为实施例三和实施例一的组合，具体可参见实施例三和实施例一，不再重复描述。

其中，图 13 中的双向鉴权命令相参见上述实施例三和实施例一中的单向鉴权命令和请求单向鉴权命令。

本申请实施例六

本实施例中，RAN 节点（接入网设备）作为读写器设备，A-IOT 设备作为标签设备，本实施例是 A-IOT 设备和 RAN 节点的双向鉴权，即 A-IOT 设备认证 RAN 节点是否合法，且 5GC 节点认证 A-IOT 设备是否合法，安全功能的对等实体为 A-IOT 设备和 5GC 节点。

参见图 14，本申请实施例的方法可视为实施例四和实施例二的组合，具体可参见实施例四和实施例二，不再重复描述。

其中，图 14 中的双向鉴权命令相参见上述实施例四和实施例二中的单向鉴权命令和请求单向鉴权命令。

本申请实施例七

本实施例中，UE（终端）作为读写器设备，A-IOT 设备作为标签设备，本实施例是 UE 对 A-IOT 设备的单向鉴权，即 UE 认证 A-IOT 设备是否合法，安全功能的对等实体为 A-IOT 设备和 UE。

请参考图 15，本申请实施例的标签设备的鉴权方法包括:

步骤 0a 和步骤 0b 为可选步骤，具体方式通过以下 1）或 2）任一项实现:

1）运营商预先通过操作管理维护（Operation Administration Maintenance，OAM）方式给所有可信 UE 预配置该运营商管控的全部或部分 A-IOT 设备的安全参数（security credential）。对于某个特定 UE，其在触发与 A-IOT 设备之间的空口安全鉴权流程之前，首先判断其预配置中是否存有该 A-IOT 设备的安全参数。

a. 若该 A-IOT 设备的安全参数在其预配置中，则可跳过步骤 0a 和步骤 0b，UE 直接触发空口的安全鉴权流程，即 UE 第一步执行图 15 中的步骤 1。

b. 若接入该 UE 的 A-IOT 设备的安全参数不在其预配置中，则 UE 在触发空口的安全鉴权流程之前，先向 5GC 节点请求该 A-IOT 设备的安全参数，请求中携带该 A-IOT 设备的标识（ID）信息，5GC 节点在判断 UE 可信的前提下，向 UE 响应该 A-IOT 设备的安全参数。即 UE 第一步执行步骤 0a，步骤 0b 是否执行取决于 5GC 节点判断 UE 是否可信。该 5GC 节点可以是相关技术中的 5GC 节点（例如接入和移动性管理功能（Access and Mobility Management Function，AMF）），或者新引入的 5GC 功能节点，在此不做限定。

2）运营商未支持通过 OAM 方式给所有可信 UE 预配置该运营商管控的全部或部分 A-IOT 设备的安全参数（security credential）的情况下，对于某个特定 UE，在触发空口的安全鉴权流程之前，总是先向 5GC 节点请求该 A-IOT 设备的安全参数，5GC 节点在判断 UE 可信的前提下，向 UE 响应该 A-IOT 设备的安全参数，即 UE 第一步执行步骤 0a，步骤 0b 是否执行取决于 5GC 节点判断 UE 是否可信。

其中，A-IOT 设备的 ID 信息，可以包括以下至少一项：A-IOT 设备的电子产品代码（Electronic Product code，EPC），A-IOT 设备的标签分配标识符（Tag identity，TID），该标签分配标识符存储在标签信息区中。标签信息区的数据在标签芯片出产时写入，写入后不能修改）。上述 ID 信息与 A-IOT 设备的出产配置保持一致，写入后不可修改。

所述 A-IOT 设备的安全参数可以包括以下至少一项：根密钥（Root key，RK）索引（通过索引值唯一确定根密钥）、通信加密算法（用于指示 A-IOT 设备支持的数据传输加密和完整性保护算法）、密钥长度、安全模式（用于指示 A-IOT 设备是否需要进行安全鉴权，安全鉴权包括进行单向鉴权还是双向鉴权，单向鉴权是 A-IOT 设备鉴权 UE 还是 UE

鉴权 A-IOT 设备、是否需要进行安全通信）、安全功能（用于指示 A-IOT 设备支持的安全鉴权算法，安全鉴权算法包括单向鉴权算法还是双向鉴权算法，单向鉴权算法是 A-IOT 设备鉴权 UE 使用的算法还是 UE 鉴权 A-IOT 设备使用的算法）、Tsec（UE 发送安全鉴权命令或安全通信命令后，等待 A-IOT 设备响应的参考时间，以 10ms 为单位）。上述安全参数与 A-IOT 设备的出产配置保持一致，写入 A-IOT 设备后不可修改。

步骤 1：UE 向 A-IOT 设备发送单向鉴权命令（即上述实施例中的第一鉴权命令），所述单向鉴权命令用于 A-IoT 设备的鉴权，所述单向鉴权命令至少携带 A-IOT 设备的安全参数的配置信息，该配置信息遵循 UE 的预配置的安全参数的内容或者遵循从 5GC 节点获取的安全参数的配置内容（即步骤 0b）。

根据步骤 1，A-IOT 设备通过计算确定 A-IOT 设备的认证码或数据签名。其中 A-IOT 设备生成 A-IOT 设备认证码或数据签名的方法，本申请不作限定。

步骤 2：A-IOT 设备向 UE 发送单向鉴权命令的响应（第一响应），所述单向鉴权命令的响应中携带：A-IOT 设备的 ID 信息，A-IOT 设备的认证码或数据签名。

根据步骤 2，UE 确定 A-IOT 设备是否通过认证，可选的，可以根据以下方法确定：

该 UE 通过确定 A-IOT 设备的认证码或数据签名，比对自己计算并生成的 A-IOT 设备的认证码或数据签名，与步骤 2 中收到的 A-IOT 设备的认证码或数据签名，如果两者取值相等，则判断 A-IOT 设备通过认证；否则，判断 A-IOT 设备认证失败。

其中 UE 计算并生成 A-IOT 设备的认证码或数据签名的方法，本申请不作限定。但须与 A-IOT 设备生成 A-IOT 设备认证码或数据签名的方法，保持一致。

进一步地，在该 UE 确定 A-IOT 设备通过认证的前提下，UE 执行以下至少一项：向 A-IOT 设备发送控制命令；

接收或处理 A-IOT 设备的数据；

转发 A-IOT 设备的数据。

这里，转发数据的对象可以是一个相关技术中的 5GC 节点，例如用户面功能（User plane Function，UPF），或者，一个新引入的 5GC 功能节点，或者 A-IOT App server 等，在此不做限定。

本申请实施例八

本实施例中，UE（终端）作为读写器设备，A-IOT 设备作为标签设备，本实施例是 A-IOT 设备对 UE 的单向鉴权，即 A-IOT 设备认证 UE 是否合法，安全功能的对等实体为 A-IOT 设备和 UE。

请参考图 16，本申请实施例的读写器设备的鉴权方法包括：

步骤 0a 和步骤 0b 同实施例七，不再重复描述。

步骤 1：UE 向 A-IOT 设备发送请求单向鉴权命令（第二鉴权命令），所述请求单向鉴权命令用于 RAN 节点的鉴权，所述请求单向鉴权命令至少携带 A-IOT 设备的安全参数的配置信息，UE 的认证码或数字签名，计算 UE 的认证码或数字签名的第二输入参数（如

UE ID，认证码或数据签名传输对应的时间信息、频域信息或波束信息中的至少一项）

在步骤 1 之前，UE 计算并生成 UE 的认证码或数据签名。其中 UE 生成 UE 设备认证码或数据签名的方法，本申请不作限定。

根据步骤 1，A-IOT 设备确定 UE 是否通过认证。可选的，可以通过以下方法确定：该 A-IOT 设备自己计算并生成 UE 的认证码或数据签名，比对自己计算并生成 UE 的认证码或数据签名，与步骤 1 中收到的 UE 的认证码或数据签名，如果两者取值相等，则判断 UE 通过认证；否则，判断 UE 认证失败。

步骤 2：A-IOT 设备向 UE 发送请求单向鉴权命令的响应，所述请求单向鉴权命令的响应至少携带 UE 是否通过认证的鉴权结果。

其中 A-IOT 设备计算并生成 UE 的认证码或数据签名的方法，本申请不作限定。但须与 UE 生成 UE 认证码或数据签名的方法，保持一致。

进一步地，在 A-IOT 设备确定该 UE 通过认证的前提下，A-IOT 设备执行以下至少一项：响应 UE 发送的其他命令；向 UE 发送 A-IOT 设备的数据。

本申请实施例九

本实施例中，UE（终端）作为读写器设备，A-IOT 设备作为标签设备，本实施例是 A-IOT 设备和 UE 的双向鉴权，即 A-IOT 设备认证 UE 是否合法，且 UE 认证 A-IOT 设备是否合法，安全功能的对等实体为 A-IOT 设备和 UE。

请参考图 17，本申请实施例的方法可视为实施例八和实施例七的组合，具体可参见实施例八和实施例七，不再重复描述。

其中，图 17 中的双向鉴权命令相参见上述实施例八和实施例七中的单向鉴权命令和请求单向鉴权命令。

本申请实施例提供的标签设备的鉴权方法，执行主体可以为标签设备的鉴权装置。本申请实施例中以标签设备的鉴权装置执行标签设备的鉴权方法为例，说明本申请实施例提供的标签设备的鉴权装置。

请参考图 18，本申请实施例还提供一种标签设备的鉴权装置 180，包括：

第一发送模块 181，用于发送第一鉴权命令，所述第一鉴权命令用于标签设备的认证，所述第一鉴权命令中包括所述标签设备的安全参数的配置信息；其中，所述标签设备的鉴权装置 180 为接入网设备、终端或核心网设备；

第一接收模块 182，用于接收第一响应，所述第一响应中包括：所述标签设备的第一认证信息；

第一确定模块 183，用于根据所述安全参数的配置信息和所述标签设备的第一认证信息，确定所述标签设备是否通过认证。

在本申请实施例中，明确了在 3GPP 系统中如何认证标签设备的流程，以使得读写器设备（终端或接入网设备）和标签设备之间的信息传输工作在安全模式。

可选的，当所述标签设备的鉴权装置 180 为接入网设备或终端时，所述安全参数存储

于所述标签设备的鉴权装置 180 中，或者，所述安全参数由所述标签设备的鉴权装置 180 从核心网设备获取。

可选的，所述标签设备的鉴权装置 180 为接入网设备或终端；

所述第一发送模块 181，用于在所述标签设备的鉴权装置 180 有所述标签设备的安全参数的情况下，发送第一鉴权命令。

可选的，所述标签设备的鉴权装置 180 为接入网设备或终端；所述标签设备的鉴权装置 180 还包括：

发送模块，用于向核心网设备发送用于获取安全参数的第一请求，所述第一请求中包括所述标签设备的标识信息；或者，在没有所述标签设备的安全参数的情况下，向核心网设备发送用于获取安全参数的第一请求，所述第一请求中包括所述标签设备的标识信息；

接收模块，用于接收来自所述核心网设备的所述安全参数。

可选的，所述标签设备的鉴权装置 180 为核心网设备；

所述第一发送模块 181，用于通过接入网设备向所述标签设备发送所述第一鉴权命令；

所述第一接收模块 182，用于接收接入网设备转发的所述第一响应；

或者

所述标签设备的鉴权装置 180 为所述标签设备的源服务小区所在的接入网设备；

所述第一发送模块 181，用于通过所述标签设备的目的服务小区所在的接入网设备向所述标签设备发送所述第一鉴权命令，其中，所述标签设备的目的服务小区所在的接入网设备转发所述第一鉴权命令；

所述第一接收模块 182，用于接收所述标签设备的目的服务小区所在的接入网设备转发的所述第一响应。

可选的，所述第一确定模块 183，用于根据所述标签设备的安全参数的配置信息和用于计算所述标签设备的第一认证信息的第一输入参数，通过计算确定所述标签设备的第二认证信息； 比较所述第二认证信息和接收到的所述标签设备的第一认证信息是否相同；若所述第二认证信息和所述第一认证信息相同，确定所述标签设备通过认证；若所述第二认证信息和所述第一认证信息不同，确定所述标签设备未通过认证。

可选的，所述标签设备的鉴权装置 180 为核心网设备时，还包括：

第二接收模块，用于接收所述标签设备的服务小区所在的接入网设备发送的所述第一输入参数。

可选的，所述第一输入参数包括以下至少一项：所述标签设备的标识信息，所述标签设备的服务小区的标识信息，所述标签设备的上下文标识，所述第一认证信息传输对应的时间信息，所述第一认证信息传输对应的频域资源信息，所述第一认证信息传输对应的波束信息。

可选的，所述标签设备的鉴权装置 180 为接入网设备或者终端，还包括：

执行模块，用于若所述标签设备通过认证，执行以下至少一项：

向所述标签设备发送控制命令;

接收所述标签设备发送的数据;

处理所述标签设备发送的数据;

转发所述标签设备发送的数据。

可选的，所述标签设备的鉴权装置 180 为核心网设备，还包括以下至少一项:

第二发送模块，用于向接入网设备或终端发送所述标签设备是否通过认证的鉴权结果;

第三发送模块，用于向接入网设备或终端发送所述标签设备的授权信息，所述授权信息在所述标签设备通过认证的情况下发送。

本申请实施例中的标签设备的鉴权装置可以是电子设备，例如具有操作系统的电子设备，也可以是电子设备中的部件，例如集成电路或芯片。该电子设备可以是终端，也可以为除终端之外的其他设备。示例性的，终端可以包括但不限于上述所列举的终端 11 的类型，其他设备可以为服务器、网络附属存储器（Network Attached Storage，NAS）等，本申请实施例不作具体限定。

本申请实施例提供的标签设备的鉴权装置能够实现图 4 的方法实施例实现的各个过程，并达到相同的技术效果，为避免重复，这里不再赘述。

请参考图 19，本申请实施例还提供一种标签设备的鉴权装置 190，包括:

第一接收模块 191，用于接收第一设备发送的第一鉴权命令，所述第一鉴权命令用于所述标签设备的认证，所述第一鉴权命令中包括所述标签设备的安全参数的配置信息;所述第一设备为接入网设备、终端或核心网设备;

第一发送模块 192，用于根据所述第一鉴权命令，向所述第一设备发送第一响应，所述第一响应中包括所述标签设备的第一认证信息。

在本申请实施例中，明确了在 3GPP 系统中如何认证标签设备的流程，，以使得读写器设备（接入网设备或终端）和标签设备之间的信息传输工作在安全模式。

可选的，当所述第一设备为接入网设备或终端时，所述安全参数存储于所述第一设备中，或者，所述安全参数由所述第一设备从核心网设备获取。

可选的，所述第一发送模块 192，用于根据所述安全参数的配置信息和用于计算所述标签设备的第一认证信息的第一输入参数，通过计算确定所述标签设备的第一认证信息;向所述第一设备发送所述第一响应，所述第一响应中包括所述第一认证信息。

可选的，所述第一输入参数包括以下至少一项:所述标签设备的标识信息，所述标签设备的服务小区的标识信息，所述标签设备的上下文标识，所述第一认证信息传输对应的时间信息，所述第一认证信息传输对应的频域资源信息，所述第一认证信息传输对应的波束信息。

本申请实施例提供的标签设备的鉴权装置能够实现图 5 的方法实施例实现的各个过程，并达到相同的技术效果，为避免重复，这里不再赘述。

本申请实施例提供的读写器设备的鉴权方法，执行主体可以为读写器设备的鉴权装置。

本申请实施例中以读写器设备的鉴权装置执行读写器设备的鉴权方法为例，说明本申请实施例提供的读写器设备的鉴权装置。

请参考图 20，本申请实施例还提供一种读写器设备的鉴权装置 200，包括：

第一发送模块 201，用于发送第二鉴权命令，所述第二鉴权命令用于读写器设备的认证，所述第二鉴权命令中包括标签设备的安全参数的配置信息和所述读写器设备的第三认证信息；其中，所述读写器设备的鉴权装置 200 为所述读写器设备或核心网设备，所述读写器设备为接入网设备或终端；

第一接收模块 202，用于接收第二响应，所述第二响应中包括：所述读写器设备通过认证或者未通过认证的鉴权结果。

在本申请实施例中，明确了在 3GPP 系统中标签设备如何认证作为读写器设备的 UE 或 RAN 的流程，以使得读写器设备和标签设备之间的信息传输工作在安全模式。

可选的，当所述第一设备为所述读写器设备时，所述安全参数存储于所述第一设备中，或者，所述安全参数由所述第一设备从核心网设备获取

可选的，所述读写器设备的鉴权装置 200 还包括：

第一确定模块，用于确定所述读写器设备的第三认证信息。

可选的，所述读写器设备的鉴权装置 200 为所述读写器设备，还包括：

第二发送模块，用于向核心网设备发送用于获取安全参数的第一请求；

或者，

第三发送模块，用于在所述第一设备没有所述标签设备的安全参数的情况下，向核心网设备发送用于获取安全参数的第一请求；其中，所述第一请求中包括所述标签设备的标识信息。

可选的，所述读写器设备的鉴权装置 200 为所述读写器设备，还包括：

第四发送模块，用于向核心网设备发送用于获取安全参数的第一请求，所述第一请求中包括所述标签设备的标识信息和用于计算所述读写器设备的第三认证信息的第二输入参数；

第二接收模块，用于接收所述核心网设备发送的所述标签设备的安全参数和所述读写器设备的第三认证信息；

或者，

第五发送模块，用于在有所述标签设备的安全参数的情况下，向核心网设备发送第二请求；所述第一设备接收所述核心网设备发送的所述读写器设备的第三认证信息；

第六发送模块，用于在没有所述标签设备的安全参数的情况下，向核心网设备发送用于获取安全参数的第一请求；所述第一设备接收所述核心网设备发送的所述标签设备的安全参数和所述读写器设备的第三认证信息；

其中，所述第一请求中包括所述标签设备的标识信息和用于计算所述读写器设备的第三认证信息的第二输入参数，所述第二请求中包括用于计算所述读写器设备的第三认证信

息的第二输入参数。

可选的，所述第二输入参数包括以下至少一项：所述第一设备的标识信息，所述第三认证信息传输对应的时间信息，所述第三认证信息传输对应的频域资源信息，所述第三认证信息传输对应的波束信息。

可选的，所述读写器设备的鉴权装置 200 为核心网设备；

所述第一发送模块 201，用于向通过接入网设备向所述标签设备发送所述第二鉴权命令；

所述第一接收模块 202，用于接收由所述接入网设备转发的所述第二响应。

可选的，所述读写器设备的鉴权装置 200 还包括：

第七发送模块，用于发送第一鉴权命令，所述第一鉴权命令用于对标签设备进行认证，所述第一鉴权命令中包括所述标签设备的安全参数的配置信息；

第三接收模块，用于接收第一响应，所述第一响应中包括：所述标签设备的第一认证信息；

第二确定模块，用于根据所述安全参数的配置信息和所述标签设备的第一认证信息，确定所述标签设备是否通过认证。

本申请实施例中的读写器设备的鉴权装置可以是电子设备，例如具有操作系统的电子设备，也可以是电子设备中的部件，例如集成电路或芯片。该电子设备可以是终端，也可以为除终端之外的其他设备。示例性的，终端可以包括但不限于上述所列举的终端 11 的类型，其他设备可以为服务器、网络附属存储器（Network Attached Storage，NAS）等，本申请实施例不作具体限定。

本申请实施例提供的读写器设备的鉴权装置能够实现图 6 的方法实施例实现的各个过程，并达到相同的技术效果，为避免重复，这里不再赘述。

请参考图 21，本申请实施例还提供一种读写器设备的鉴权装置 210，包括：

第一接收模块 211，用于接收第一设备发送的第二鉴权命令，所述第二鉴权命令用于读写器设备的认证，所述第二鉴权命令中包括所述标签设备的安全参数的配置信息和所述读写器设备的第三认证信息；其中，所述第一设备为所述读写器设备或核心网设备，所述读写器设备为接入网设备或终端；

第一确定模块 212，用于根据所述第二鉴权命令，确定所述读写器设备是否通过认证。

在本申请实施例中，明确了在 3GPP 系统中标签设备如何认证作为读写器设备的 UE 或 RAN 的流程，以使得读写器设备和标签设备之间的信息传输工作在安全模式。

可选的，当所述第一设备为所述读写器设备时，所述安全参数存储于所述第一设备中，或者，所述安全参数由所述第一设备从核心网设备获取。

可选的，所述第一确定模块 212，用于根据所述标签设备的安全参数的配置信息和用于计算所述读写器设备的第三认证信息的第二输入参数，通过计算确定所述读写器设备的第四认证信息；比较所述第四认证信息和接收到的所述读写器设备的第三认证信息是否

相同；若所述第四认证信息和所述第三认证信息相同，确定所述读写器设备通过认证；若所述第四认证信息和所述第三认证信息不同，确定所述读写器设备未通过认证。

可选的，所述第二输入参数包括以下至少一项：所述第一设备的标识信息，所述第三认证信息传输对应的时间信息，所述第三认证信息传输对应的频域资源信息，所述第三认证信息传输对应的波束信息。

可选的，所述读写器设备的鉴权装置 210 还包括：

执行模块，用于若所述读写器设备通过认证，执行以下至少一项：

向所述第一设备发送第二响应，所述第二响应中包括：所述读写器设备通过认证或者未通过认证的鉴权结果；

响应所述读写器设备发送的控制命令；

向所述读写器设备发送数据。

可选的，所述读写器设备的鉴权装置 210 还包括：

第二接收模块，用于接收所述第一设备发送的第一鉴权命令，所述第一鉴权命令用于对所述标签设备进行认证，所述第一鉴权命令中包括所述标签设备的安全参数的配置信息；

第二确定模块，用于根据所述第一鉴权命令，确定所述标签设备的第一认证信息；

发送模块，用于向所述第一设备发送第一响应，所述第一响应中包括：所述标签设备的第一认证信息。

可选的，所述读写器设备的鉴权装置 210 还包括：

丢弃模块，用于若所述读写器设备未通过认证，丢弃所述第一设备发送的第一鉴权命令，所述第一鉴权命令用于对所述标签设备进行认证，所述第一鉴权命令中包括所述标签设备的安全参数的配置信息。

本申请实施例提供的读写器设备的鉴权装置能够实现图 7 的方法实施例实现的各个过程，并达到相同的技术效果，为避免重复，这里不再赘述。

本申请实施例提供的安全鉴权方法，执行主体可以为安全鉴权装置。本申请实施例中以安全鉴权装置执行安全鉴权方法为例，说明本申请实施例提供的安全鉴权装置。

请参考图 22，本申请实施例还提供一种安全鉴权装置 220，包括：

第一接收模块 221，用于接收读写器设备发送的请求，所述请求中包括标签设备的标识信息和/或用于计算所述读写器设备的认证信息的第二输入参数；所述读写器设备为接入网设备或终端；

第一发送模块 222，用于向所述读写器设备发送所述标签设备的安全参数和/或所述读写器设备的第三认证信息，其中，所述第三认证信息由所述核心网设备根据所述标签设备的安全参数和所述第二输入参数通过计算确定。

本申请实施例中，作为读写器设备的接入网设备或终端在对标签设备进行鉴权之前，或者，请求标签设备对所述读写器设备进行鉴权之前，可以向核心网设备获取标签设备的安全参数和/或请求核心网设备确定读写器设备的认证信息，核心网设备验证读写器设备

可信的情况下，再向读写器设备发送所述标签设备的安全参数和/或读写器设备的认证信息，从而保证参与鉴权的接入网设备或终端是可信的设备。

可选的，所述第一发送模块，用于在判断所述读写器设备可信的情况下，向所述读写器设备发送所述标签设备的安全参数和/或所述读写器设备的第三认证信息。

本申请实施例中的安全鉴权装置可以是电子设备，例如具有操作系统的电子设备，也可以是电子设备中的部件，例如集成电路或芯片。

本申请实施例提供的安全鉴权装置能够实现图 8 的方法实施例实现的各个过程，并达到相同的技术效果，为避免重复，这里不再赘述。

如图 23 所示，本申请实施例还提供一种通信设备 230，包括处理器 231 和存储器 232，存储器 232 上存储有可在所述处理器 231 上运行的程序或指令，例如，该通信设备 230 为第一设备时，该程序或指令被处理器 231 执行时实现上述第一设备执行的方法实施例的各个步骤，且能达到相同的技术效果。该通信设备 230 为标签设备时，该程序或指令被处理器 231 执行时实现上述标签设备执行的方法实施例的各个步骤，且能达到相同的技术效果。该通信设备 230 为核心网设备时，该程序或指令被处理器 231 执行时实现上述核心网设备执行的方法实施例的各个步骤，且能达到相同的技术效果。为避免重复，这里不再赘述。

本申请实施例还提供一种终端，包括处理器和通信接口，所述通信接口和所述处理器耦合，所述处理器用于运行程序或指令，实现如图 4 或图 6 所示方法实施例中的步骤。该终端实施例与上述第一设备侧执行的方法实施例对应，上述方法实施例的各个实施过程和实现方式均可适用于该终端实施例中，且能达到相同的技术效果。具体地，图 24 为实现本申请实施例的一种终端的硬件结构示意图。

该终端 240 包括但不限于：射频单元 241、网络模块 242、音频输出单元 243、输入单元 244、传感器 245、显示单元 246、用户输入单元 247、接口单元 248、存储器 249 以及处理器 2410 等中的至少部分部件。

本领域技术人员可以理解，终端 240 还可以包括给各个部件供电的电源（比如电池），电源可以通过电源管理系统与处理器 2410 逻辑相连，从而通过电源管理系统实现管理充电、放电以及功耗管理等功能。图 24 中示出的终端结构并不构成对终端的限定，终端可以包括比图示更多或更少的部件，或者组合某些部件，或者不同的部件布置，在此不再赘述。

应理解的是，本申请实施例中，输入单元 244 可以包括图形处理器（Graphics Processing Unit，GPU）2441 和麦克风 2442，图形处理器 2441 对在视频捕获模式或图像捕获模式中由图像捕获装置（如摄像头）获得的静态图片或视频的图像数据进行处理。显示单元 246 可包括显示面板 2461，可以采用液晶显示器、有机发光二极管等形式来配置显示面板 2461。用户输入单元 247 包括触控面板 2471 以及其他输入设备 2472 中的至少一种。触控面板 2471，也称为触摸屏。触控面板 2471 可包括触摸检测装置和触摸控制器两个部分。其他输入设备 2472 可以包括但不限于物理键盘、功能键（比如音量控制按键、开关按键等）、

轨迹球、鼠标、操作杆，在此不再赘述。

本申请实施例中，射频单元 241 接收来自网络侧设备的下行数据后，可以传输给处理器 2410 进行处理；另外，射频单元 241 可以向网络侧设备发送上行数据。通常，射频单元 241 包括但不限于天线、放大器、收发信机、耦合器、低噪声放大器、双工器等。

存储器 249 可用于存储软件程序或指令以及各种数据。存储器 249 可主要包括存储程序或指令的第一存储区和存储数据的第二存储区，其中，第一存储区可存储操作系统、至少一个功能所需的应用程序或指令（比如声音播放功能、图像播放功能等）等。此外，存储器 249 可以包括易失性存储器或非易失性存储器。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），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（Synch link DRAM，SLDRAM）和直接内存总线随机存取存储器（Direct Rambus RAM，DRRAM）。本申请实施例中的存储器 249 包括但不限于这些和任意其它适合类型的存储器。

处理器 2410 可包括一个或多个处理单元；可选的，处理器 2410 集成应用处理器和调制解调处理器，其中，应用处理器主要处理涉及操作系统、用户界面和应用程序等的操作，调制解调处理器主要处理无线通信信号，如基带处理器。可以理解的是，上述调制解调处理器也可以不集成到处理器 2410 中。

其中，在一个实施例中，射频单元 241，用于发送第一鉴权命令，所述第一鉴权命令用于标签设备的认证，所述第一鉴权命令中包括所述标签设备的安全参数的配置信息；接收第一响应，所述第一响应中包括：所述标签设备的第一认证信息；

处理器 2410，用于根据所述安全参数的配置信息和所述标签设备的第一认证信息，确定所述标签设备是否通过认证。

在本申请实施例中，明确了在 3GPP 系统中如何认证标签设备的流程，以使得读写器设备（终端或接入网设备）和标签设备之间的信息传输工作在安全模式。

可以理解，本实施例中提及的各实现方式的实现过程可以参照方法实施例 4 的相关描述，并达到相同或相应的技术效果，为避免重复，在此不再赘述。

或者，在另一个实施例中，射频单元 241，用于发送第二鉴权命令，所述第二鉴权命令用于读写器设备的认证，所述第二鉴权命令中包括标签设备的安全参数的配置信息和所述读写器设备的第三认证信息；接收第二响应，所述第二响应中包括：所述读写器设备通过认证或者未通过认证的鉴权结果。

在本申请实施例中，明确了在 3GPP 系统中标签设备如何认证作为读写器设备的 UE 或 RAN 的流程，以使得读写器设备和标签设备之间的信息传输工作在安全模式。

可以理解，本实施例中提及的各实现方式的实现过程可以参照方法实施例 6 的相关描述，并达到相同或相应的技术效果，为避免重复，在此不再赘述。

本申请实施例还提供一种网络侧设备，包括处理器和通信接口，所述通信接口和所述处理器耦合，所述处理器用于运行程序或指令，实现如图 4 或图 6 所示的方法实施例的步骤。该网络侧设备实施例与上述第一设备侧方法实施例对应，上述方法实施例的各个实施过程和实现方式均可适用于该网络侧设备实施例中，且能达到相同的技术效果。

具体地，本申请实施例还提供了一种网络侧设备。如图 25 所示，该网络侧设备 2500 包括：天线 251、射频装置 252、基带装置 253、处理器 254 和存储器 255。天线 251 与射频装置 252 连接。在上行方向上，射频装置 252 通过天线 251 接收信息，将接收的信息发送给基带装置 253 进行处理。在下行方向上，基带装置 253 对要发送的信息进行处理，并发送给射频装置 252，射频装置 252 对收到的信息进行处理后经过天线 251 发送出去。

以上实施例中网络侧设备执行的方法可以在基带装置 253 中实现，该基带装置 253 包括基带处理器。

基带装置 253 例如可以包括至少一个基带板，该基带板上设置有多个芯片，如图 25 所示，其中一个芯片例如为基带处理器，通过总线接口与存储器 255 连接，以调用存储器 255 中的程序，执行以上方法实施例中所示的网络设备操作。

该网络侧设备还可以包括网络接口 256，该接口例如为通用公共无线接口（Common Public Radio Interface，CPRI）。

具体地，本申请实施例的网络侧设备 2500 还包括：存储在存储器 255 上并可在处理器 254 上运行的指令或程序，处理器 254 调用存储器 255 中的指令或程序执行图 18 或图 20 所示各模块执行的方法，并达到相同的技术效果，为避免重复，故不在此赘述。

具体地，本申请实施例还提供了一种网络侧设备。如图 26 所示，该网络侧设备 260 包括：处理器 261、网络接口 262 和存储器 263。其中，网络接口 262 例如为通用公共无线接口（common public radio interface，CPRI）。

具体地，本申请实施例的网络侧设备 260 还包括：存储在存储器 263 上并可在处理器 261 上运行的指令或程序，处理器 261 调用存储器 263 中的指令或程序执行图 18 或图 20 或图 22 所示各模块执行的方法，并达到相同的技术效果，为避免重复，故不在此赘述。

本申请实施例还提供一种可读存储介质，所述可读存储介质上存储有程序或指令，该程序或指令被处理器执行时实现上述方法实施例的各个过程，且能达到相同的技术效果，为避免重复，这里不再赘述。

其中，所述处理器为上述实施例中所述的终端中的处理器。所述可读存储介质，包括计算机可读存储介质，如计算机只读存储器 ROM、随机存取存储器 RAM、磁碟或者光盘等。在一些示例中，可读存储介质可以是非瞬态的可读存储介质。

本申请实施例另提供了一种芯片，所述芯片包括处理器和通信接口，所述通信接口和所述处理器耦合，所述处理器用于运行程序或指令，实现上述方法实施例的各个过程，且能达到相同的技术效果，为避免重复，这里不再赘述。

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。

本申请实施例另提供了一种计算机程序/程序产品，所述计算机程序/程序产品被存储在存储介质中，所述计算机程序/程序产品被至少一个处理器执行以实现上述方法实施例的各个过程，且能达到相同的技术效果，为避免重复，这里不再赘述。

本申请实施例还提供了一种无线通信系统，包括：第一设备和标签设备，所述第一设备可用于执行如上述第一设备侧执行的所述的方法的步骤，所述标签设备可用于执行如上述标签设备侧执行的所述的方法的步骤。

本申请实施例还提供了一种无线通信系统，包括：第一设备、标签设备和核心网设备，所述第一设备可用于执行如上述第一设备侧所述的方法的步骤，所述标签设备可用于执行如上述标签设备侧所述的方法的步骤，所述核心网设备可用于执行如上述核心网设备侧所述的方法的步骤。

需要说明的是，在本文中，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、物品或者装置不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、物品或者装置所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括该要素的过程、方法、物品或者装置中还存在另外的相同要素。此外，需要指出的是，本申请实施方式中的方法和装置的范围不限按示出或讨论的顺序来执行功能，还可包括根据所涉及的功能按基本同时的方式或按相反的顺序来执行功能，例如，可以按不同于所描述的次序来执行所描述的方法，并且还可以添加、省去或组合各种步骤。另外，参照某些示例所描述的特征可在其他示例中被组合。

通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到上述实施例方法可借助计算机软件产品加必需的通用硬件平台的方式来实现，当然也可以通过硬件。该计算机软件产品存储在存储介质（如ROM、RAM、磁碟、光盘等）中，包括若干指令，用以使得终端或者网络侧设备执行本申请各个实施例所述的方法。

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

权 利 要 求 书

1. 一种标签设备的鉴权方法，包括:

第一设备发送第一鉴权命令，所述第一鉴权命令用于标签设备的认证，所述第一鉴权命令中包括所述标签设备的安全参数的配置信息；其中，所述第一设备为接入网设备、终端或核心网设备;

所述第一设备接收第一响应，所述第一响应中包括：所述标签设备的第一认证信息;

所述第一设备根据所述安全参数的配置信息和所述标签设备的第一认证信息，确定所述标签设备是否通过认证。

2. 根据权利要求 1 所述的方法，其中，当所述第一设备为接入网设备或终端时，所述安全参数存储于所述第一设备中，或者，所述安全参数由所述第一设备从核心网设备获取。

3. 根据权利要求 1 所述的方法，其中，所述第一设备为接入网设备或终端;

所述第一设备发送第一鉴权命令，包括：在所述第一设备有所述标签设备的安全参数的情况下，所述第一设备发送第一鉴权命令。

4. 根据权利要求 1 所述的方法，其中，所述第一设备为接入网设备或终端;

在所述第一设备发送第一鉴权命令之前，还包括:

所述第一设备向核心网设备发送用于获取安全参数的第一请求，所述第一请求中包括所述标签设备的标识信息；或者，在所述第一设备没有所述标签设备的安全参数的情况下，所述第一设备向核心网设备发送用于获取安全参数的第一请求，其中，所述第一请求中包括所述标签设备的标识信息;

所述第一设备接收来自所述核心网设备的所述安全参数。

5. 根据权利要求 1 所述的方法，其中，

所述第一设备为核心网设备;

所述第一设备发送第一鉴权命令包括：所述第一设备通过接入网设备向所述标签设备发送所述第一鉴权命令;

所述第一设备接收第一响应包括：所述第一设备接收接入网设备转发的所述第一响应;

或者

所述第一设备为所述标签设备的源服务小区所在的接入网设备;

所述第一设备发送第一鉴权命令包括：所述第一设备通过所述标签设备的目的服务小区所在的接入网设备向所述标签设备发送所述第一鉴权命令，其中，所述标签设备的目的服务小区所在的接入网设备转发所述第一鉴权命令;

所述第一设备接收第一响应包括：所述第一设备接收所述标签设备的目的服务小区所在的接入网设备转发的所述第一响应。

6. 根据权利要求 1 所述的方法，其中，所述第一设备根据所述安全参数的配置信息和所述标签设备的第一认证信息，确定所述标签设备是否通过认证，包括:

所述第一设备根据所述标签设备的安全参数的配置信息和用于计算所述标签设备的第一认证信息的第一输入参数，通过计算确定所述标签设备的第二认证信息；

所述第一设备比较所述第二认证信息和接收到的所述标签设备的第一认证信息是否相同；

若所述第二认证信息和所述第一认证信息相同，确定所述标签设备通过认证；

若所述第二认证信息和所述第一认证信息不同，确定所述标签设备未通过认证。

7. 根据权利要求 6 所述的方法，其中，当所述第一设备为核心网设备时，所述第一设备根据第一输入参数以及所述标签设备的安全参数的配置信息，通过计算确定所述标签设备的第一认证信息之前还包括：

所述第一设备接收所述标签设备的服务小区所在的接入网设备发送的所述第一输入参数。

8. 根据权利要求 6 或 7 所述的方法，其中，所述第一输入参数包括以下至少一项：所述标签设备的标识信息，所述标签设备的服务小区的标识信息，所述标签设备的上下文标识，所述第一认证信息传输对应的时间信息，所述第一认证信息传输对应的频域资源信息，所述第一认证信息传输对应的波束信息。

9. 根据权利要求 1 或 6 所述的方法，其中，所述第一设备为接入网设备或者终端，所述确定所述标签设备是否通过认证之后还包括：

若所述标签设备通过认证，所述第一设备执行以下至少一项：

向所述标签设备发送控制命令；

接收所述标签设备发送的数据；

处理所述标签设备发送的数据；

转发所述标签设备发送的数据。

10. 根据权利要求 1 或 6 所述的方法，其中，所述第一设备为核心网设备，所述确定所述标签设备是否通过认证之后还包括以下至少一项：

所述第一设备向接入网设备或终端发送所述标签设备是否通过认证的鉴权结果；

所述第一设备向接入网设备或终端发送所述标签设备的授权信息，所述授权信息在所述标签设备通过认证的情况下发送。

11. 一种标签设备的鉴权方法，包括：

标签设备接收第一设备发送的第一鉴权命令，所述第一鉴权命令用于所述标签设备的认证，所述第一鉴权命令中包括所述标签设备的安全参数的配置信息；所述第一设备为接入网设备、终端或核心网设备；

所述标签设备根据所述第一鉴权命令，向所述第一设备发送第一响应，所述第一响应中包括所述标签设备的第一认证信息。

12. 根据权利要求 11 所述的方法，其中，当所述第一设备为接入网设备或终端时，所述安全参数存储于所述第一设备中，或者，所述安全参数由所述第一设备从核心网设备获

取。

13. 根据权利要求 11 所述的方法，其中，所述标签设备根据所述第一鉴权命令，向所述第一设备发送第一响应，包括:

所述标签设备根据所述安全参数的配置信息和用于计算所述标签设备的第一认证信息的第一输入参数，通过计算确定所述标签设备的第一认证信息;

所述标签设备向所述第一设备发送所述第一响应，所述第一响应中包括所述第一认证信息。

14. 根据权利要求 13 所述的方法，其中，所述第一输入参数包括以下至少一项：所述标签设备的标识信息，所述标签设备的服务小区的标识信息，所述标签设备的上下文标识，所述第一认证信息传输对应的时间信息，所述第一认证信息传输对应的频域资源信息，所述第一认证信息传输对应的波束信息。

15. 一种读写器设备的鉴权方法，包括:

第一设备发送第二鉴权命令，所述第二鉴权命令用于读写器设备的认证，所述第二鉴权命令中包括标签设备的安全参数的配置信息和所述读写器设备的第三认证信息；其中，所述第一设备为所述读写器设备或核心网设备，所述读写器设备为接入网设备或终端;

所述第一设备接收第二响应，所述第二响应中包括：所述读写器设备通过认证或者未通过认证的鉴权结果。

16. 根据权利要求 15 所述的方法，其中，当所述第一设备为所述读写器设备时，所述安全参数存储于所述第一设备中，或者，所述安全参数由所述第一设备从核心网设备获取。

17. 根据权利要求 15 或 16 所述的方法，其中，所述第一设备发送第二鉴权命令之前还包括:

所述第一设备确定所述读写器设备的第三认证信息。

18. 根据权利要求 15 或 16 所述的方法，其中，所述第一设备为所述读写器设备，所述第一设备发送第二鉴权命令之前还包括:

所述第一设备向核心网设备发送用于获取安全参数的第一请求;

或者，

在所述第一设备没有所述标签设备的安全参数的情况下，所述第一设备向核心网设备发送用于获取安全参数的第一请求;

其中，所述第一请求中包括所述标签设备的标识信息。

19. 根据权利要求 15 或 16 所述的方法，其中，所述第一设备为读写器设备，所述第一设备发送第二鉴权命令之前还包括:

所述第一设备向核心网设备发送用于获取安全参数的第一请求，所述第一请求中包括所述标签设备的标识信息和用于计算所述读写器设备的第三认证信息的第二输入参数;

所述第一设备接收所述核心网设备发送的所述标签设备的安全参数和所述读写器设备的第三认证信息;

或者，

在所述第一设备有所述标签设备的安全参数的情况下，所述第一设备向核心网设备发送第二请求；所述第一设备接收所述核心网设备发送的所述读写器设备的第三认证信息；

在所述第一设备没有所述标签设备的安全参数的情况下，所述第一设备向核心网设备发送用于获取安全参数的第一请求；所述第一设备接收所述核心网设备发送的所述标签设备的安全参数和所述读写器设备的第三认证信息；

其中，所述第一请求中包括所述标签设备的标识信息和用于计算所述读写器设备的第三认证信息的第二输入参数，所述第二请求中包括用于计算所述读写器设备的第三认证信息的第二输入参数。

20. 根据权利要求 19 所述的方法，其中，所述第二输入参数包括以下至少一项：所述第一设备的标识信息，所述第三认证信息传输对应的时间信息，所述第三认证信息传输对应的频域资源信息，所述第三认证信息传输对应的波束信息。

21. 根据权利要求 15 所述的方法，其中，所述第一设备为核心网设备；

所述第一设备发送第二鉴权命令包括：所述第一设备向通过接入网设备向所述标签设备发送所述第二鉴权命令；

所述第一设备接收第二响应包括：所述第一设备接收由所述接入网设备转发的所述第二响应。

22. 根据权利要求 15 所述的方法，其中，所述第一设备接收第二响应之后还包括：

所述第一设备发送第一鉴权命令，所述第一鉴权命令用于对标签设备进行认证，所述第一鉴权命令中包括所述标签设备的安全参数的配置信息；

所述第一设备接收第一响应，所述第一响应中包括：所述标签设备的第一认证信息；

所述第一设备根据所述安全参数的配置信息和所述标签设备的第一认证信息，确定所述标签设备是否通过认证。

23. 一种读写器设备的鉴权方法，包括：

标签设备接收第一设备发送的第二鉴权命令，所述第二鉴权命令用于读写器设备的认证，所述第二鉴权命令中包括所述标签设备的安全参数的配置信息和所述读写器设备的第三认证信息；其中，所述第一设备为所述读写器设备或核心网设备，所述读写器设备为接入网设备或终端；

所述标签设备根据所述第二鉴权命令，确定所述读写器设备是否通过认证。

24. 根据权利要求 23 所述的方法，其中，

当所述第一设备为所述读写器设备时，所述安全参数存储于所述第一设备中，或者，所述安全参数由所述第一设备从核心网设备获取。

25. 根据权利要求 23 所述的方法，其中，所述标签设备根据所述第二鉴权命令，确定所述读写器设备是否通过认证，包括：

所述标签设备根据所述标签设备的安全参数的配置信息和用于计算所述读写器设备

的第三认证信息的第二输入参数，通过计算确定所述读写器设备的第四认证信息；

所述标签设备比较所述第四认证信息和接收到的所述读写器设备的第三认证信息是否相同；

若所述第四认证信息和所述第三认证信息相同，确定所述读写器设备通过认证；

若所述第四认证信息和所述第三认证信息不同，确定所述读写器设备未通过认证。

26. 根据权利要求 25 所述的方法，其中，所述第二输入参数包括以下至少一项：所述第一设备的标识信息，所述第三认证信息传输对应的时间信息，所述第三认证信息传输对应的频域资源信息，所述第三认证信息传输对应的波束信息。

27. 根据权利要求 23 所述的方法，其中，所述标签设备根据所述第二鉴权命令，确定所述读写器设备是否通过认证之后还包括：

若所述读写器设备通过认证，所述标签设备执行以下至少一项：

向所述第一设备发送第二响应，所述第二响应中包括：所述读写器设备通过认证或者未通过认证的鉴权结果；

响应所述读写器设备发送的控制命令；

向所述读写器设备发送数据。

28. 根据权利要求 23 所述的方法，其中，所述标签设备接收第一设备发送的第二鉴权命令之后还包括：

所述标签设备接收所述第一设备发送的第一鉴权命令，所述第一鉴权命令用于对所述标签设备进行认证，所述第一鉴权命令中包括所述标签设备的安全参数的配置信息；

所述标签设备根据所述第一鉴权命令，确定所述标签设备的第一认证信息；

所述标签设备向所述第一设备发送第一响应，所述第一响应中包括：所述标签设备的第一认证信息。

29. 根据权利要求 23 所述的方法，其中，所述标签设备根据所述第二鉴权命令，确定所述读写器设备是否通过认证之后还包括：

若所述读写器设备未通过认证，所述标签设备丢弃所述第一设备发送的第一鉴权命令，所述第一鉴权命令用于对所述标签设备进行认证，所述第一鉴权命令中包括所述标签设备的安全参数的配置信息。

30. 一种安全鉴权方法，包括：

核心网设备接收读写器设备发送的请求，所述请求中包括标签设备的标识信息和/或用于计算所述读写器设备的认证信息的第二输入参数；所述读写器设备为接入网设备或终端；

所述核心网设备向所述读写器设备发送所述标签设备的安全参数和/或所述读写器设备的第三认证信息，其中，所述第三认证信息由所述核心网设备根据所述标签设备的安全参数和所述第二输入参数通过计算确定。

31. 根据权利要求 30 所述的方法，其中，所述核心网设备向所述读写器设备发送所述

标签设备的安全参数和/或所述读写器设备的第三认证信息包括:

所述核心网设备在判断所述读写器设备可信的情况，向所述读写器设备发送所述标签设备的安全参数和/或所述读写器设备的第三认证信息。

32. 一种标签设备的鉴权装置，包括:

第一发送模块，用于发送第一鉴权命令，所述第一鉴权命令用于标签设备的认证，所述第一鉴权命令中包括所述标签设备的安全参数的配置信息；其中，所述标签设备的鉴权装置为接入网设备、终端或核心网设备;

第一接收模块，用于接收第一响应，所述第一响应中包括：所述标签设备的第一认证信息;

第一确定模块，用于根据所述安全参数的配置信息和所述标签设备的第一认证信息，确定所述标签设备是否通过认证。

33. 一种标签设备的鉴权装置，包括:

第一接收模块，用于接收第一设备发送的第一鉴权命令，所述第一鉴权命令用于所述标签设备的认证，所述第一鉴权命令中包括所述标签设备的安全参数的配置信息；所述第一设备为接入网设备、终端或核心网设备;

第一发送模块，用于根据所述第一鉴权命令，向所述第一设备发送第一响应，所述第一响应中包括所述标签设备的第一认证信息。

34. 一种读写器设备的鉴权装置，包括:

第一发送模块，用于发送第二鉴权命令，所述第二鉴权命令用于读写器设备的认证，所述第二鉴权命令中包括标签设备的安全参数的配置信息和所述读写器设备的第三认证信息；其中，所述读写器设备的鉴权装置为所述读写器设备或核心网设备，所述读写器设备为接入网设备或终端;

第一接收模块，用于接收第二响应，所述第二响应中包括：所述读写器设备通过认证或者未通过认证的鉴权结果。

35. 一种读写器设备的鉴权装置，包括:

第一接收模块，用于接收第一设备发送的第二鉴权命令，所述第二鉴权命令用于读写器设备的认证，所述第二鉴权命令中包括标签设备的安全参数的配置信息和所述读写器设备的第三认证信息；其中，所述第一设备为所述读写器设备或核心网设备，所述读写器设备为接入网设备或终端;

第一确定模块，用于根据所述第二鉴权命令，确定所述读写器设备是否通过认证。

36. 一种安全鉴权装置，包括:

第一接收模块，用于接收读写器设备发送的请求，所述请求中包括标签设备的标识信息和/或用于计算所述读写器设备的认证信息的第二输入参数；所述读写器设备为接入网设备或终端;

第一发送模块，用于在向所述读写器设备发送所述标签设备的安全参数和/或所述读

写器设备的第三认证信息，其中，所述第三认证信息根据所述标签设备的安全参数和所述第二输入参数通过计算确定。

37. 一种通信设备，包括处理器和存储器，所述存储器存储可在所述处理器上运行的程序或指令，所述程序或指令被所述处理器执行时实现如权利要求 1 至 10 任一项所述的标签设备的鉴权方法的步骤，或者，所述程序或指令被所述处理器执行时实现如权利要求 11 至 14 任一项所述的标签设备的鉴权方法的步骤，或者，所述程序或指令被所述处理器执行时实现如权利要求 15 至 22 任一项所述的读写器设备的鉴权方法的步骤，或者，所述程序或指令被所述处理器执行时实现如权利要求 23 至 29 任一项所述的读写器设备的鉴权方法的步骤，或者，所述程序或指令被所述处理器执行时实现如权利要求 30 至 31 任一项所述的安全鉴权方法的步骤。

38. 一种可读存储介质，所述可读存储介质上存储程序或指令，所述程序或指令被处理器执行时实现如权利要求 1 至 10 任一项所述的标签设备的鉴权方法的步骤，或者，实现如权利要求 11 至 14 任一项所述的标签设备的鉴权方法的步骤，或者，实现如权利要求 15 至 22 任一项所述的读写器设备的鉴权方法的步骤，或者，实现如权利要求 23 至 29 任一项所述的读写器设备的鉴权方法的步骤，或者，实现如权利要求 30 至 31 任一项所述的安全鉴权方法的步骤。

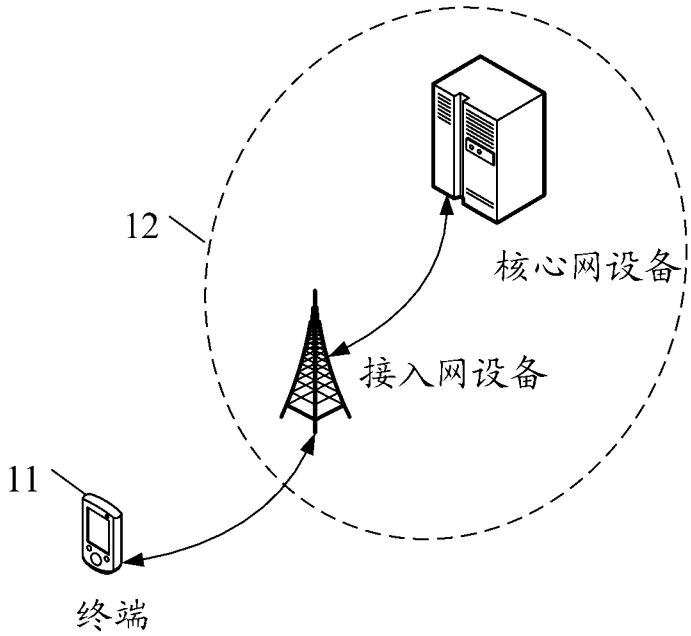
12
核心网设备
接入网设备
11
终端

图 1

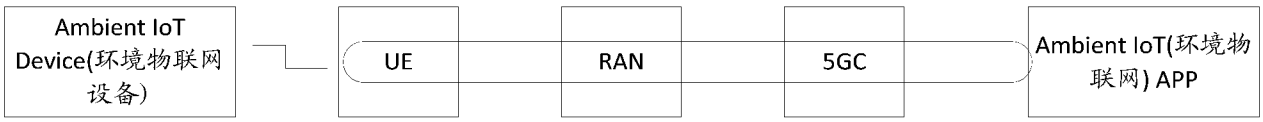
Ambient IoT Device(环境物联网设备)
UE
RAN
5GC
Ambient IoT(环境物联网) APP

图 2

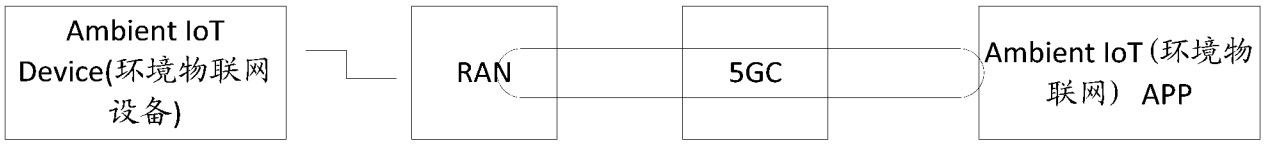
Ambient IoT Device(环境物联网设备)
RAN
5GC
Ambient IoT（环境物联网） APP

图 3

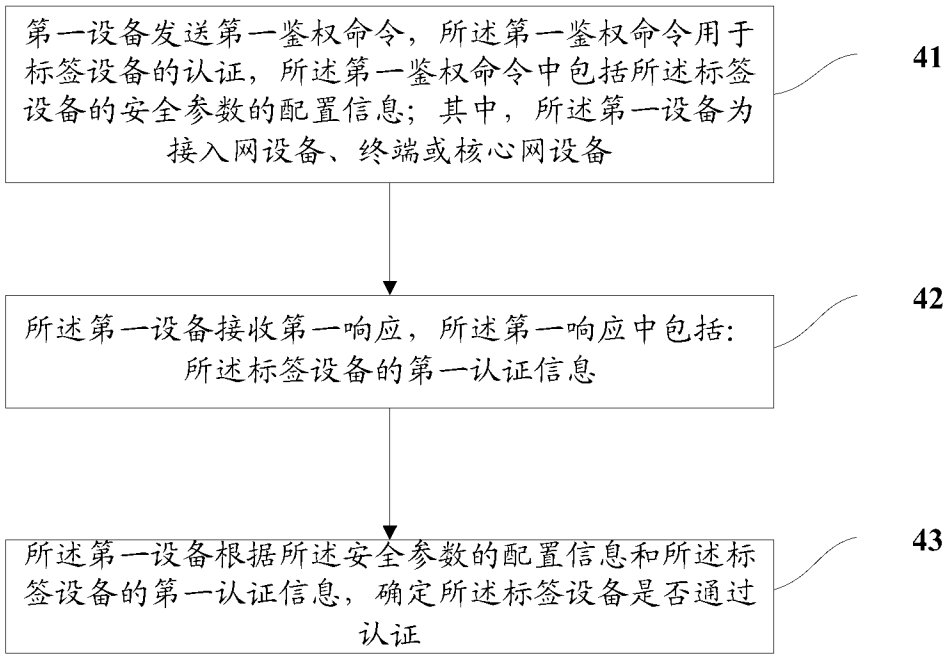
第一设备发送第一鉴权命令，所述第一鉴权命令用于标签设备的认证，所述第一鉴权命令中包括所述标签设备的安全参数的配置信息；其中，所述第一设备为接入网设备、终端或核心网设备
41
所述第一设备接收第一响应，所述第一响应中包括：所述标签设备的第一认证信息
42
所述第一设备根据所述安全参数的配置信息和所述标签设备的第一认证信息，确定所述标签设备是否通过认证
43

图 4

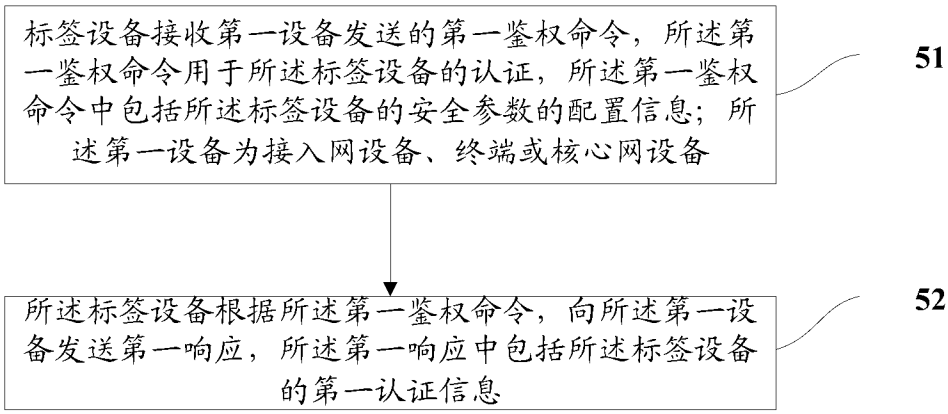
标签设备接收第一设备发送的第一鉴权命令，所述第一鉴权命令用于所述标签设备的认证，所述第一鉴权命令中包括所述标签设备的安全参数的配置信息；所述第一设备为接入网设备、终端或核心网设备
51
所述标签设备根据所述第一鉴权命令，向所述第一设备发送第一响应，所述第一响应中包括所述标签设备的第一认证信息
52

图 5

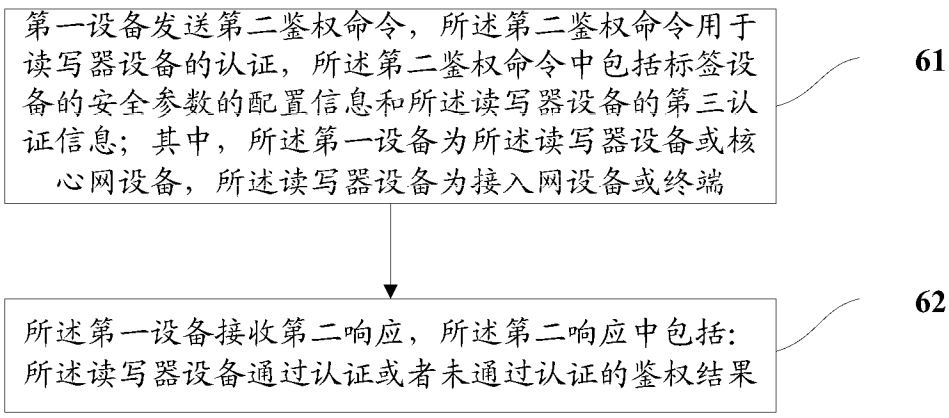
第一设备发送第二鉴权命令，所述第二鉴权命令用于读写器设备的认证，所述第二鉴权命令中包括标签设备的安全参数的配置信息和所述读写器设备的第三认证信息；其中，所述第一设备为所述读写器设备或核心网设备，所述读写器设备为接入网设备或终端
61
所述第一设备接收第二响应，所述第二响应中包括：所述读写器设备通过认证或者未通过认证的鉴权结果
62

图 6

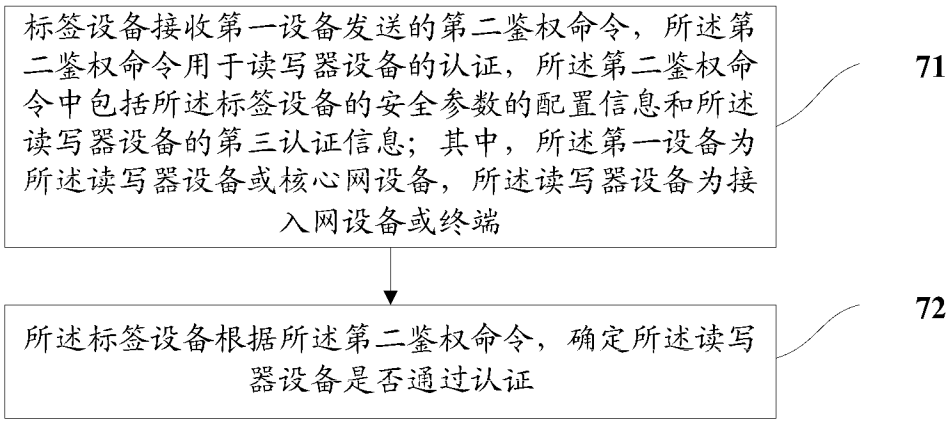
标签设备接收第一设备发送的第二鉴权命令，所述第二鉴权命令用于读写器设备的认证，所述第二鉴权命令中包括所述标签设备的安全参数的配置信息和所述读写器设备的第三认证信息；其中，所述第一设备为所述读写器设备或核心网设备，所述读写器设备为接入网设备或终端
71
所述标签设备根据所述第二鉴权命令，确定所述读写器设备是否通过认证
72

图 7

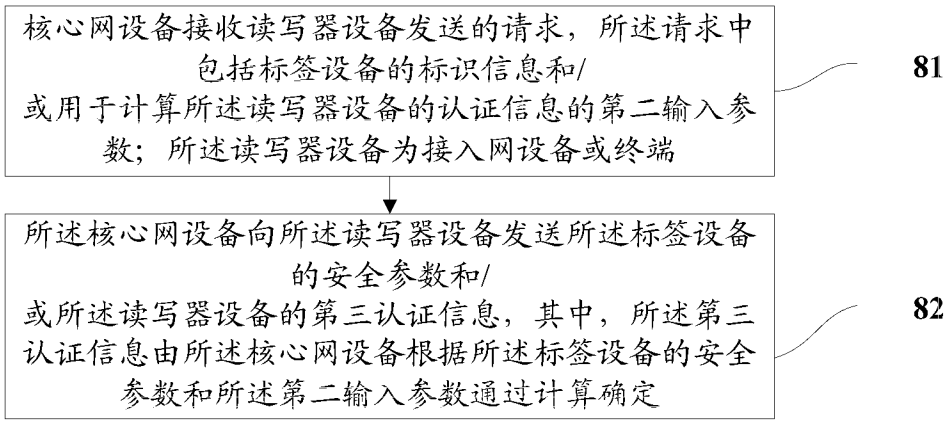
核心网设备接收读写器设备发送的请求，所述请求中包括标签设备的标识信息和/
或用于计算所述读写器设备的认证信息的第二输入参数；所述读写器设备为接入网设备或终端
81
所述核心网设备向所述读写器设备发送所述标签设备的安全参数和/
或所述读写器设备的第三认证信息，其中，所述第三认证信息由所述核心网设备根据所述标签设备的安全参数和所述第二输入参数通过计算确定
82

图 8

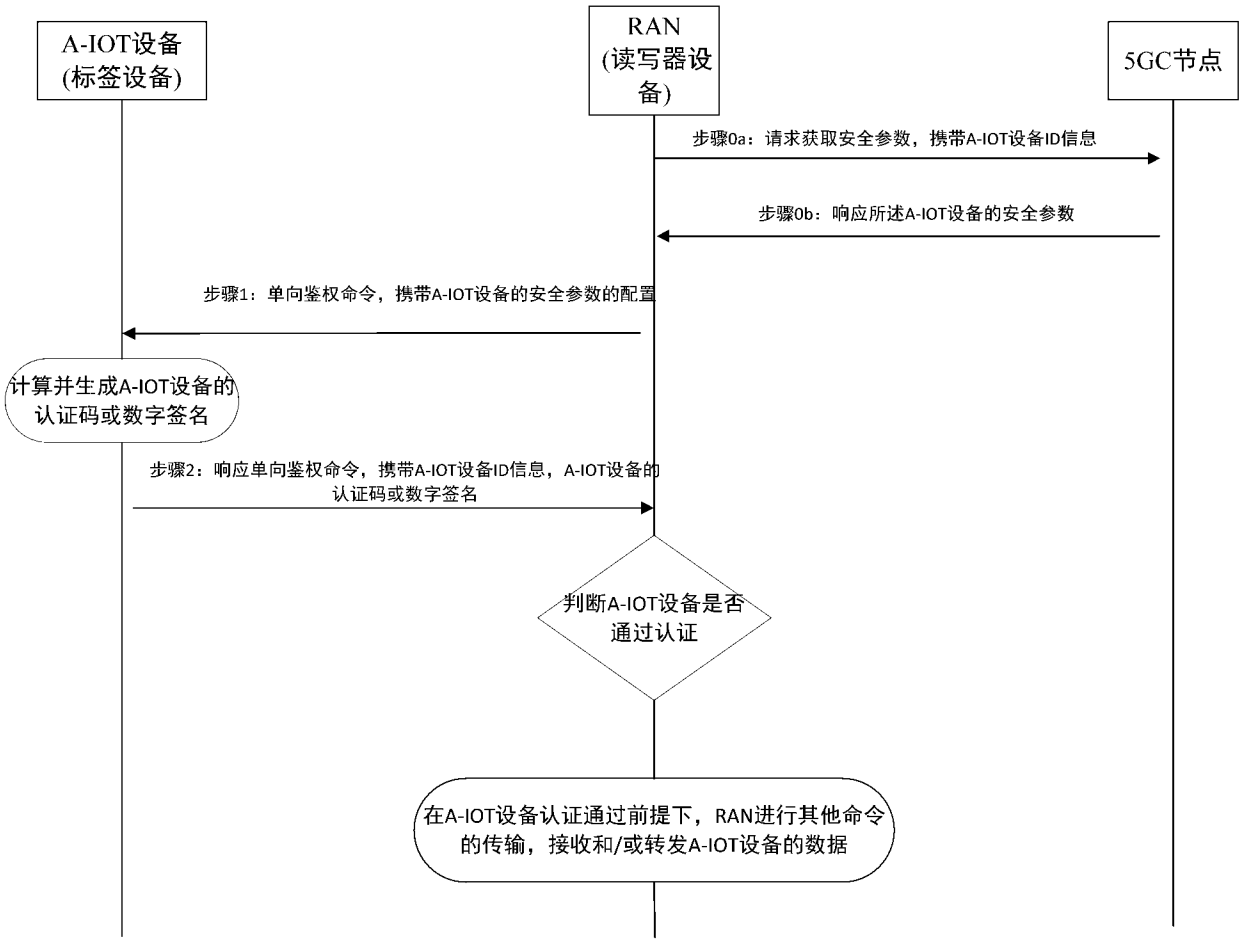
A-IOT设备
(标签设备)
RAN
(读写器设备)
5GC节点
步骤0a：请求获取安全参数，携带A-IOT设备ID信息
步骤0b：响应所述A-IOT设备的安全参数
步骤1：单向鉴权命令，携带A-IOT设备的安全参数的配置
计算并生成A-IOT设备的认证码或数字签名
步骤2：响应单向鉴权命令，携带A-IOT设备ID信息，A-IOT设备的认证码或数字签名
判断A-IOT设备是否通过认证
在A-IOT设备认证通过前提下，RAN进行其他命令的传输，接收和/或转发A-IOT设备的数据

图 9

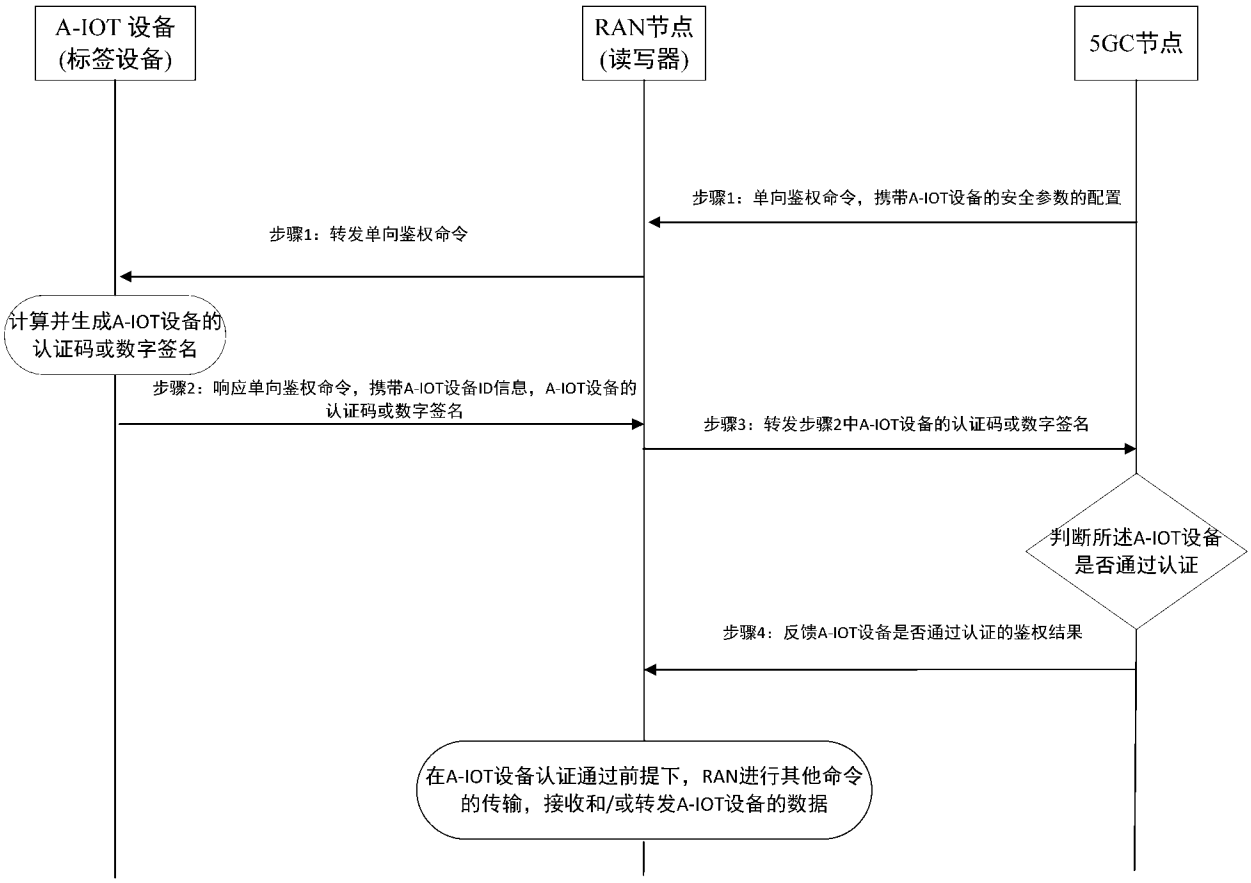
A-IOT 设备
(标签设备)
RAN节点
(读写器)
5GC节点
步骤1：单向鉴权命令，携带A-IOT设备的安全参数的配置
步骤1：转发单向鉴权命令
计算并生成A-IOT设备的
认证码或数字签名
步骤2：响应单向鉴权命令，携带A-IOT设备ID信息，A-IOT设备的
认证码或数字签名
步骤3：转发步骤2中A-IOT设备的认证码或数字签名
判断所述A-IOT设备
是否通过认证
步骤4：反馈A-IOT设备是否通过认证的鉴权结果
在A-IOT设备认证通过前提下，RAN进行其他命令
的传输，接收和/或转发A-IOT设备的数据

图 10

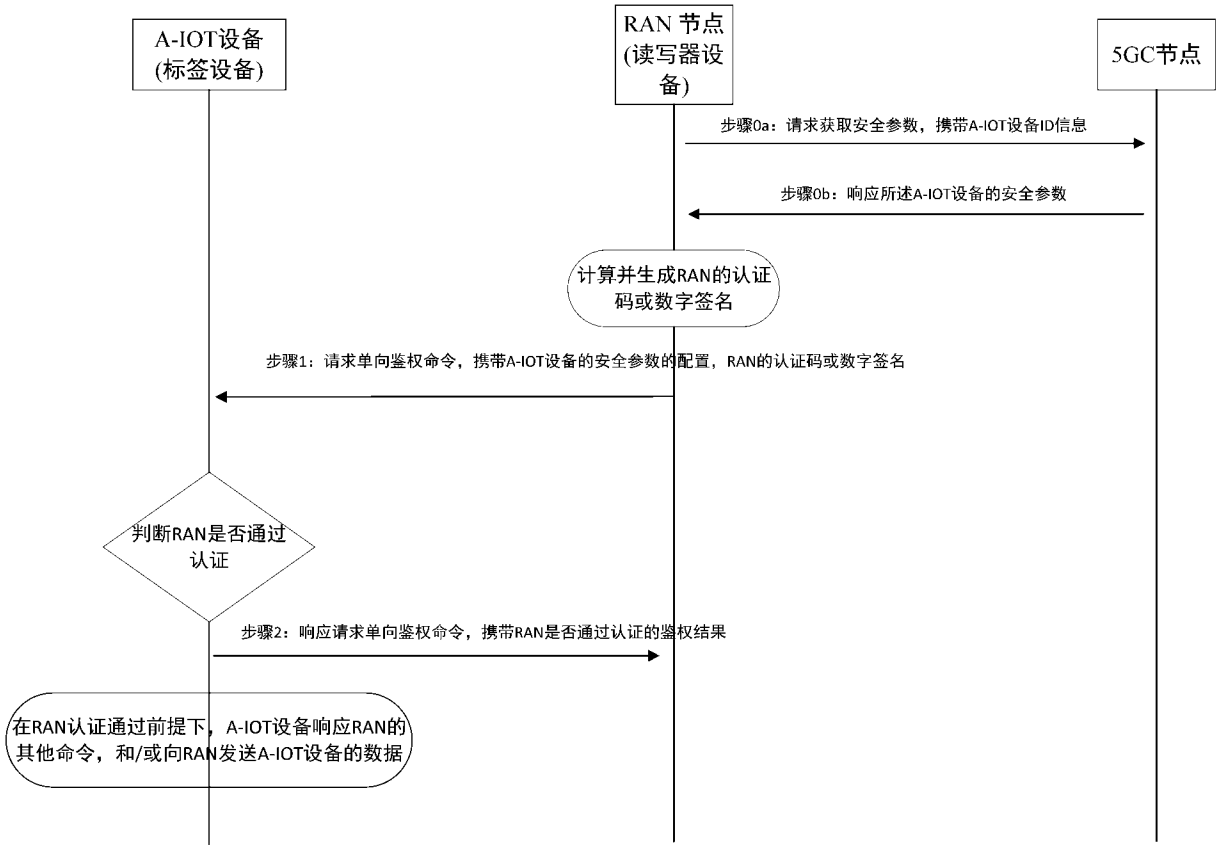
A-IOT设备
(标签设备)
RAN 节点
(读写器设
备)
5GC节点
步骤0a：请求获取安全参数，携带A-IOT设备ID信息
步骤0b：响应所述A-IOT设备的安全参数
计算并生成RAN的认证
码或数字签名
步骤1：请求单向鉴权命令，携带A-IOT设备的安全参数的配置，RAN的认证码或数字签名
判断RAN是否通过
认证
步骤2：响应请求单向鉴权命令，携带RAN是否通过认证的鉴权结果
在RAN认证通过前提下，A-IOT设备响应RAN的
其他命令，和/或向RAN发送A-IOT设备的数据

图 11

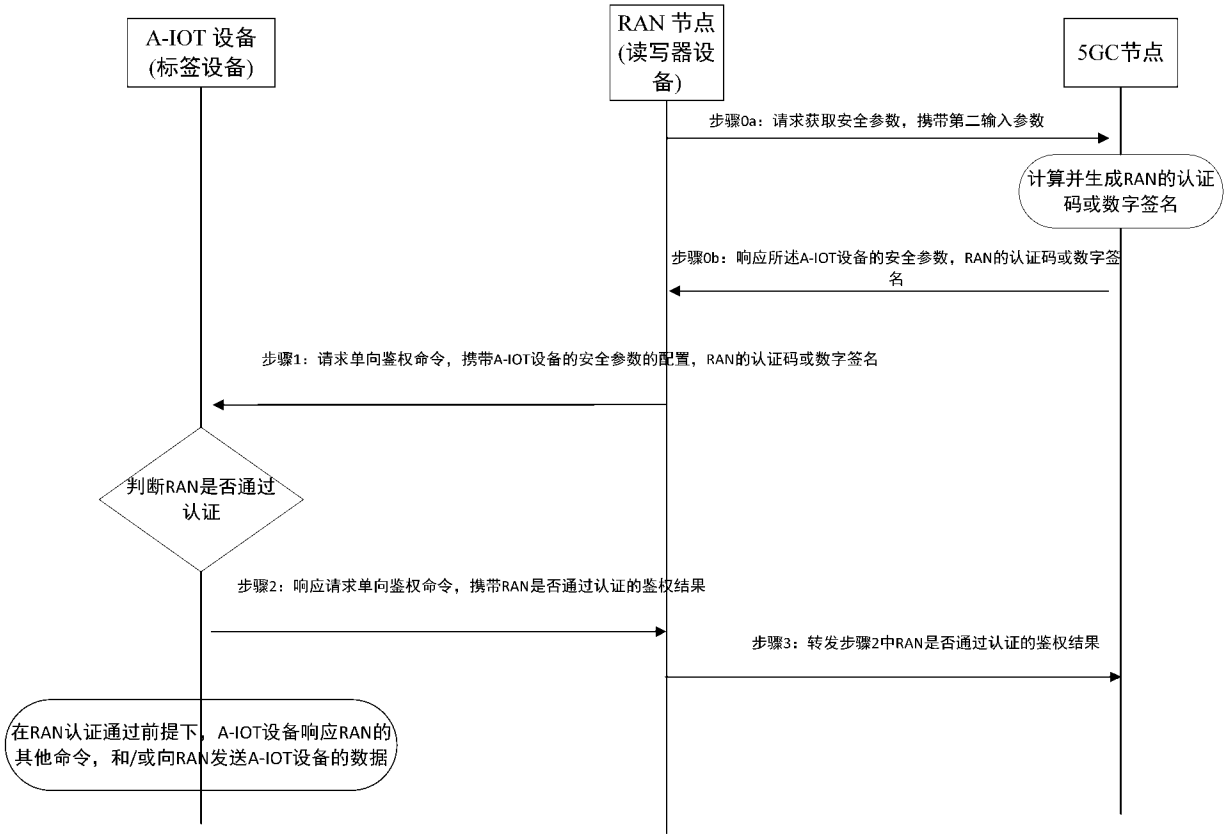
A-IOT 设备
(标签设备)
RAN 节点
(读写器设备)
5GC节点
步骤0a：请求获取安全参数，携带第二输入参数
计算并生成RAN的认证码或数字签名
步骤0b：响应所述A-IOT设备的安全参数，RAN的认证码或数字签名
步骤1：请求单向鉴权命令，携带A-IOT设备的安全参数的配置，RAN的认证码或数字签名
判断RAN是否通过认证
步骤2：响应请求单向鉴权命令，携带RAN是否通过认证的鉴权结果
步骤3：转发步骤2中RAN是否通过认证的鉴权结果
在RAN认证通过前提下，A-IOT设备响应RAN的其他命令，和/或向RAN发送A-IOT设备的数据

图 12

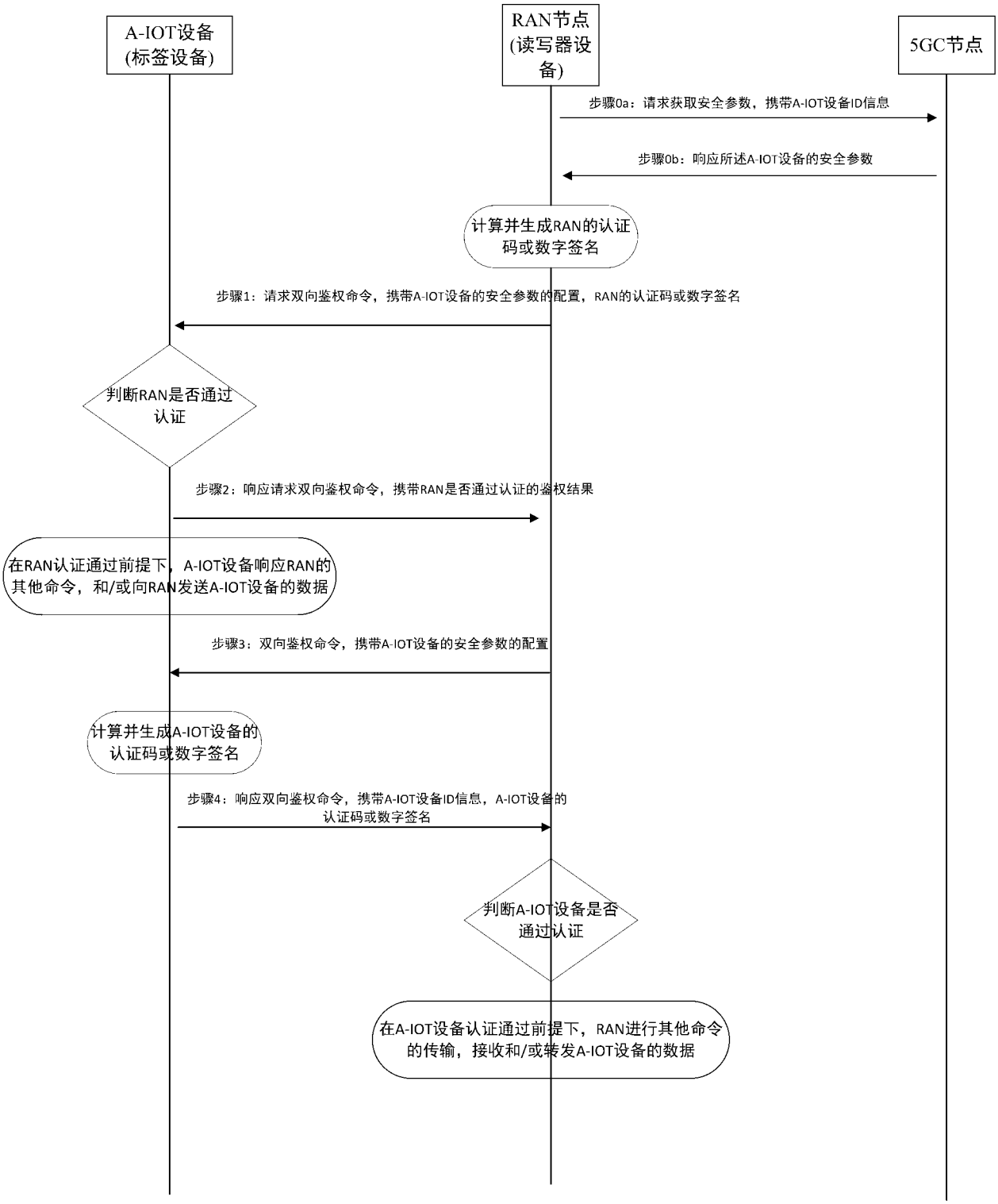
A-IOT设备
(标签设备)
RAN节点
(读写器设备)
5GC节点
步骤0a：请求获取安全参数，携带A-IOT设备ID信息
步骤0b：响应所述A-IOT设备的安全参数
计算并生成RAN的认证码或数字签名
步骤1：请求双向鉴权命令，携带A-IOT设备的安全参数的配置，RAN的认证码或数字签名
判断RAN是否通过认证
步骤2：响应请求双向鉴权命令，携带RAN是否通过认证的鉴权结果
在RAN认证通过前提下，A-IOT设备响应RAN的其他命令，和/或向RAN发送A-IOT设备的数据
步骤3：双向鉴权命令，携带A-IOT设备的安全参数的配置
计算并生成A-IOT设备的认证码或数字签名
步骤4：响应双向鉴权命令，携带A-IOT设备ID信息，A-IOT设备的认证码或数字签名
判断A-IOT设备是否通过认证
在A-IOT设备认证通过前提下，RAN进行其他命令的传输，接收和/或转发A-IOT设备的数据

图 13

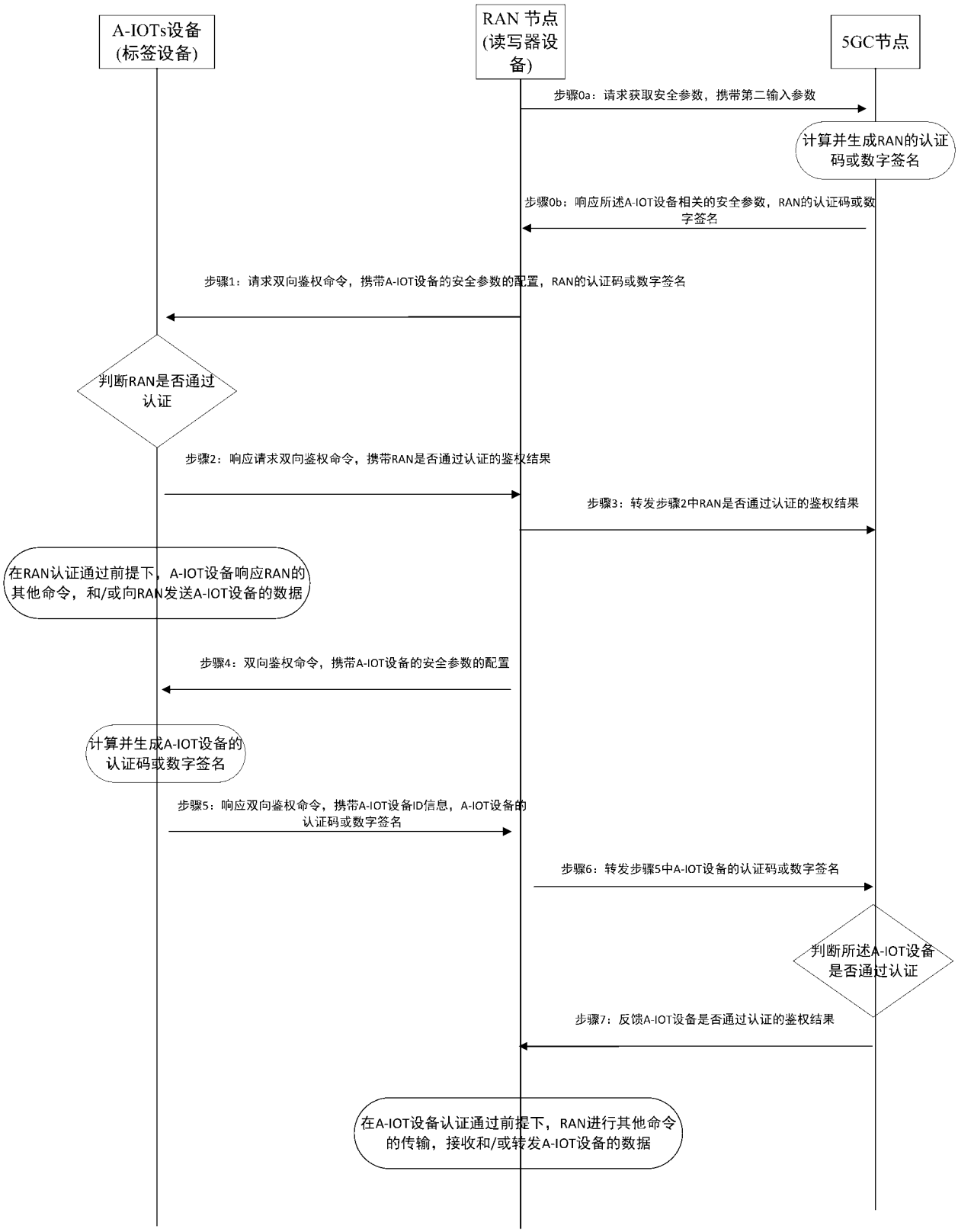
A-IOTs设备
(标签设备)
RAN 节点
(读写器设备)
5GC节点
步骤0a：请求获取安全参数，携带第二输入参数
计算并生成RAN的认证码或数字签名
步骤0b：响应所述A-IOT设备相关的安全参数，RAN的认证码或数字签名
步骤1：请求双向鉴权命令，携带A-IOT设备的安全参数的配置，RAN的认证码或数字签名
判断RAN是否通过认证
步骤2：响应请求双向鉴权命令，携带RAN是否通过认证的鉴权结果
步骤3：转发步骤2中RAN是否通过认证的鉴权结果
在RAN认证通过前提下，A-IOT设备响应RAN的其他命令，和/或向RAN发送A-IOT设备的数据
步骤4：双向鉴权命令，携带A-IOT设备的安全参数的配置
计算并生成A-IOT设备的认证码或数字签名
步骤5：响应双向鉴权命令，携带A-IOT设备ID信息，A-IOT设备的认证码或数字签名
步骤6：转发步骤5中A-IOT设备的认证码或数字签名
判断所述A-IOT设备是否通过认证
步骤7：反馈A-IOT设备是否通过认证的鉴权结果
在A-IOT设备认证通过前提下，RAN进行其他命令的传输，接收和/或转发A-IOT设备的数据

图 14

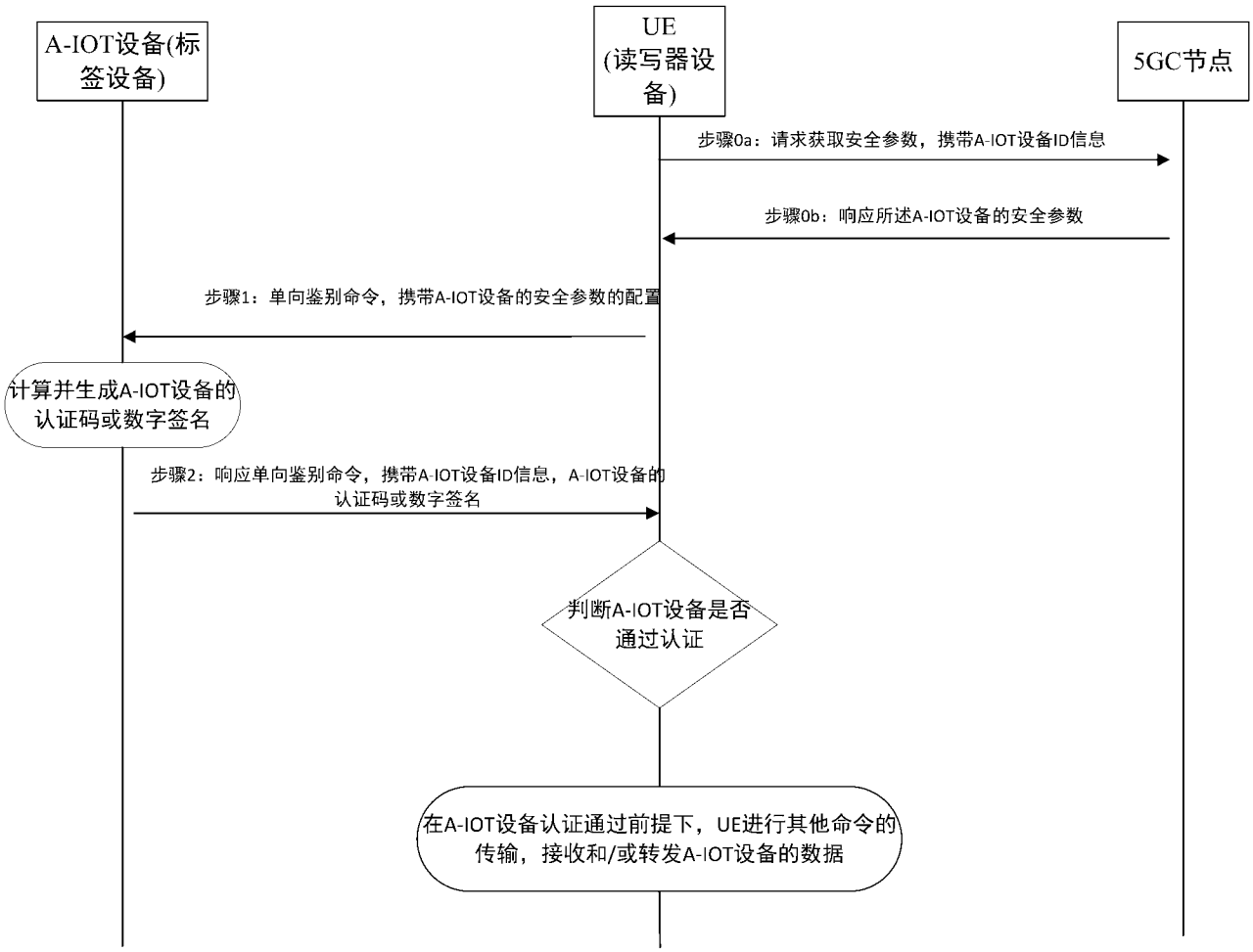
A-IOT设备(标签设备)
UE(读写器设备)
5GC节点
步骤0a：请求获取安全参数，携带A-IOT设备ID信息
步骤0b：响应所述A-IOT设备的安全参数
步骤1：单向鉴别命令，携带A-IOT设备的安全参数的配置
计算并生成A-IOT设备的认证码或数字签名
步骤2：响应单向鉴别命令，携带A-IOT设备ID信息，A-IOT设备的认证码或数字签名
判断A-IOT设备是否通过认证
在A-IOT设备认证通过前提下，UE进行其他命令的传输，接收和/或转发A-IOT设备的数据

图 15

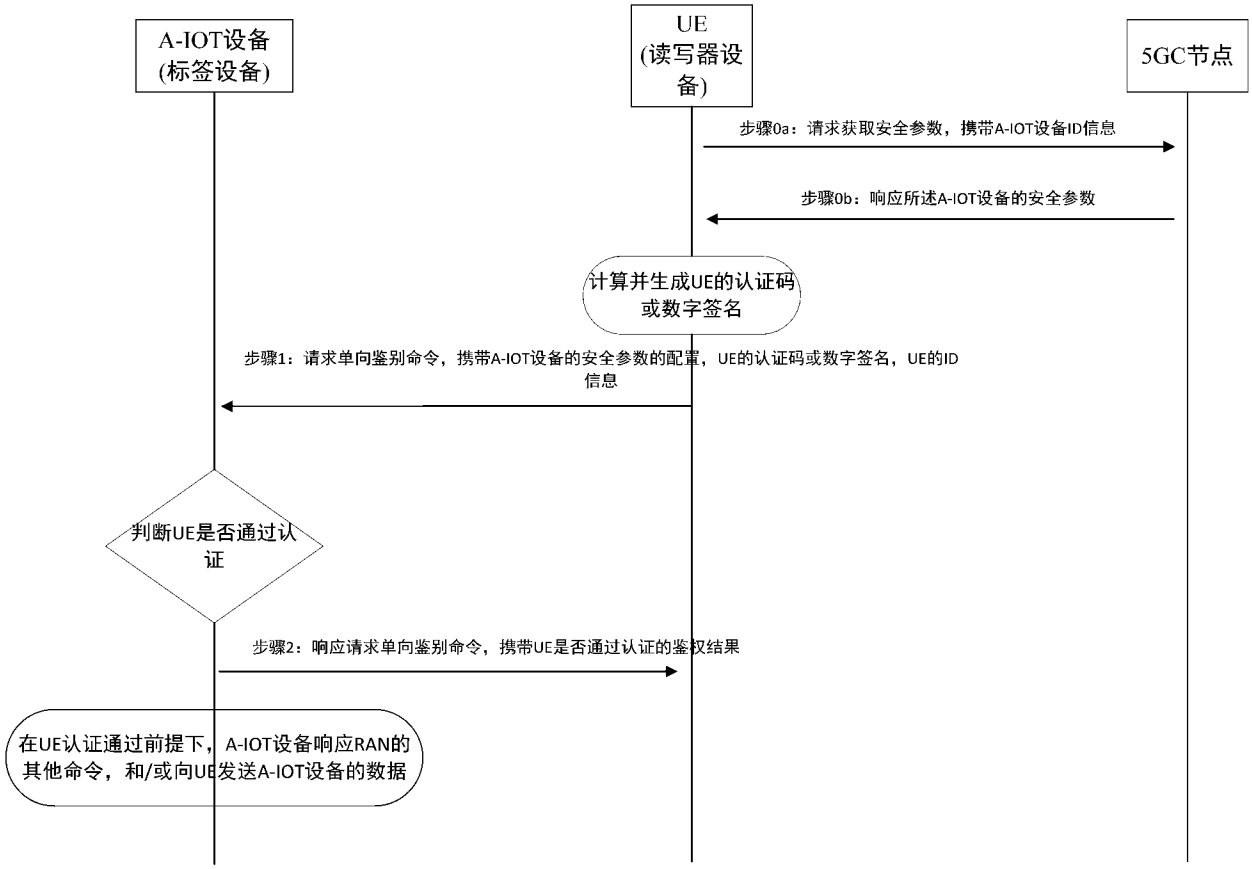
A-IOT设备
(标签设备)
UE
(读写器设备)
5GC节点
步骤0a：请求获取安全参数，携带A-IOT设备ID信息
步骤0b：响应所述A-IOT设备的安全参数
计算并生成UE的认证码或数字签名
步骤1：请求单向鉴别命令，携带A-IOT设备的安全参数的配置，UE的认证码或数字签名，UE的ID信息
判断UE是否通过认证
步骤2：响应请求单向鉴别命令，携带UE是否通过认证的鉴权结果
在UE认证通过前提下，A-IOT设备响应RAN的其他命令，和/或向UE发送A-IOT设备的数据

图 16

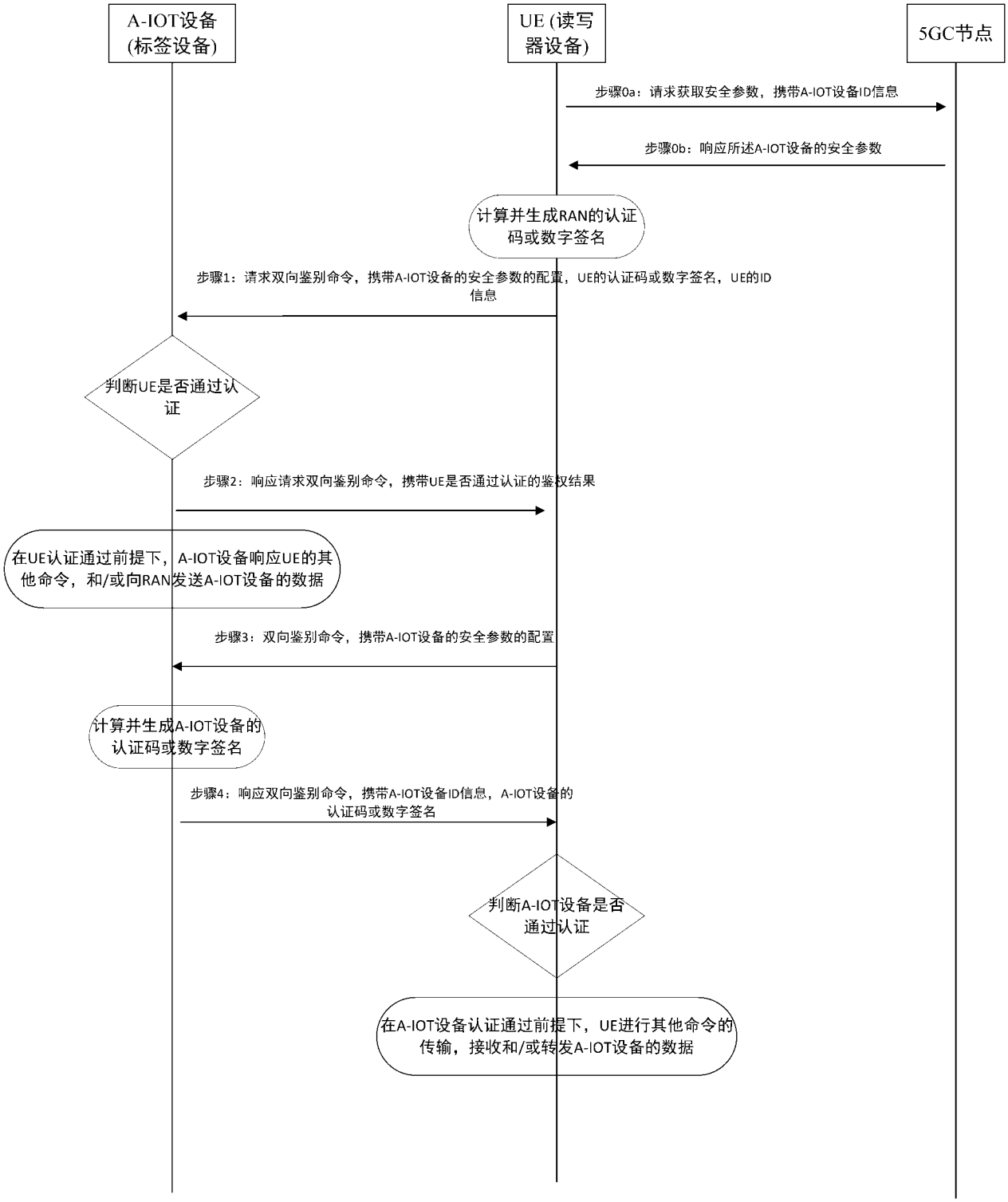
A-IOT设备
(标签设备)
UE (读写
器设备)
5GC节点
步骤0a：请求获取安全参数，携带A-IOT设备ID信息
步骤0b：响应所述A-IOT设备的安全参数
计算并生成RAN的认证
码或数字签名
步骤1：请求双向鉴别命令，携带A-IOT设备的安全参数的配置，UE的认证码或数字签名，UE的ID
信息
判断UE是否通过认
证
步骤2：响应请求双向鉴别命令，携带UE是否通过认证的鉴权结果
在UE认证通过前提下，A-IOT设备响应UE的其
他命令，和/或向RAN发送A-IOT设备的数据
步骤3：双向鉴别命令，携带A-IOT设备的安全参数的配置
计算并生成A-IOT设备的
认证码或数字签名
步骤4：响应双向鉴别命令，携带A-IOT设备ID信息，A-IOT设备的
认证码或数字签名
判断A-IOT设备是否
通过认证
在A-IOT设备认证通过前提下，UE进行其他命令的
传输，接收和/或转发A-IOT设备的数据

图 17

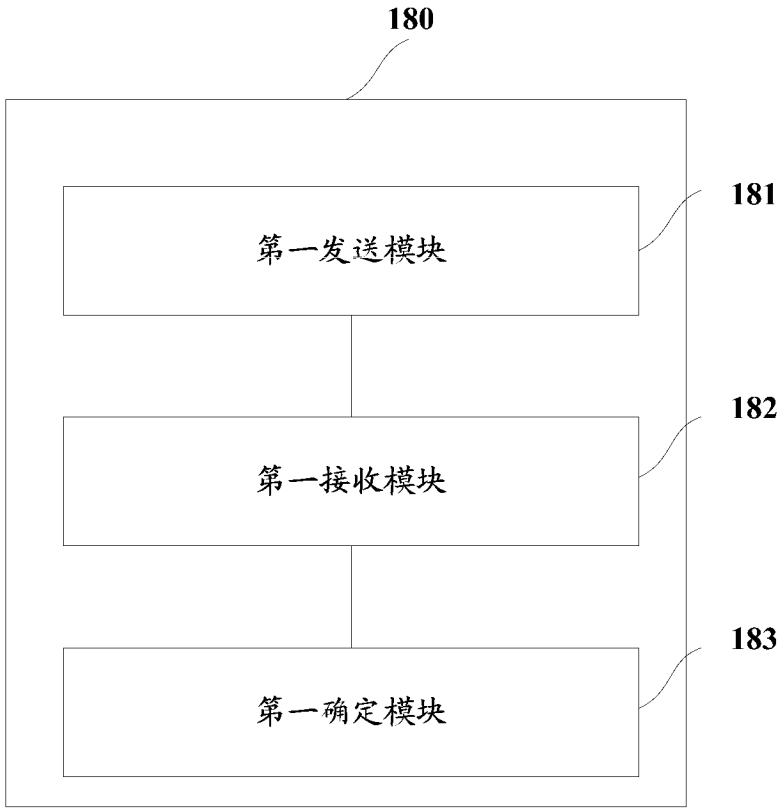
180
第一发送模块
181
第一接收模块
182
第一确定模块
183

图 18

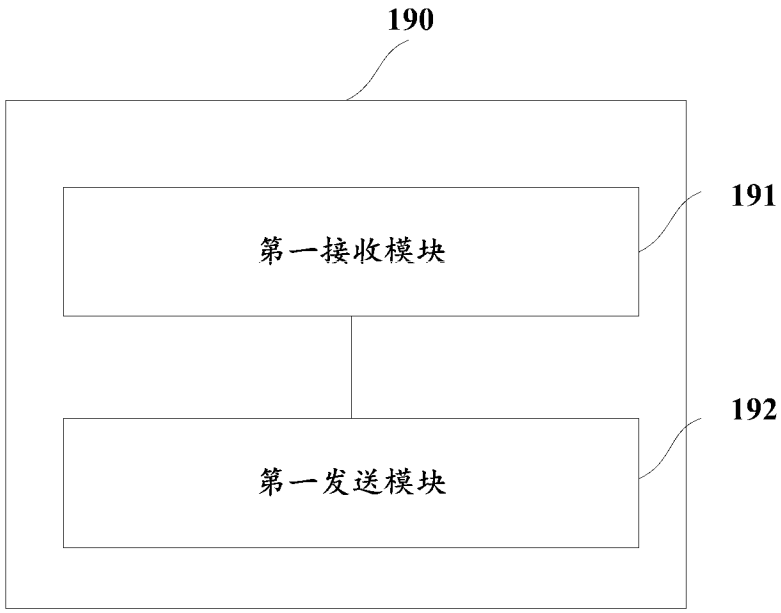
190
第一接收模块
191
第一发送模块
192

图 19

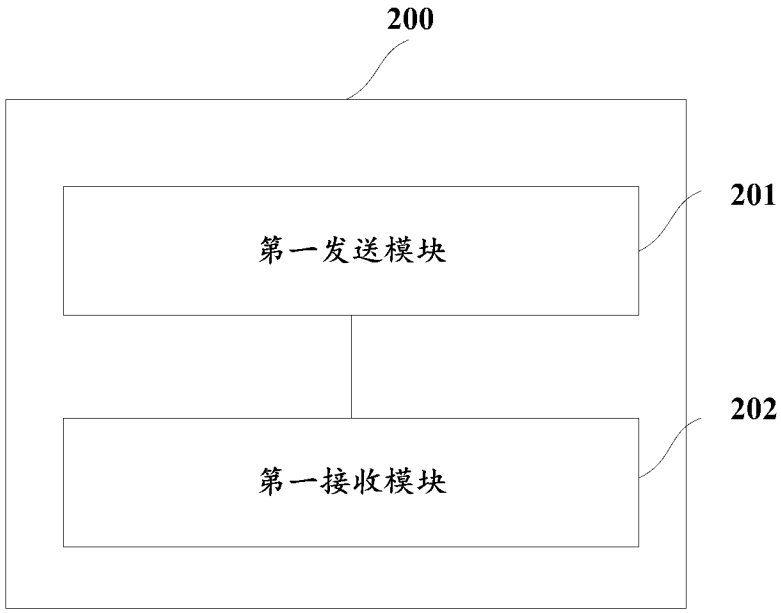

图 20

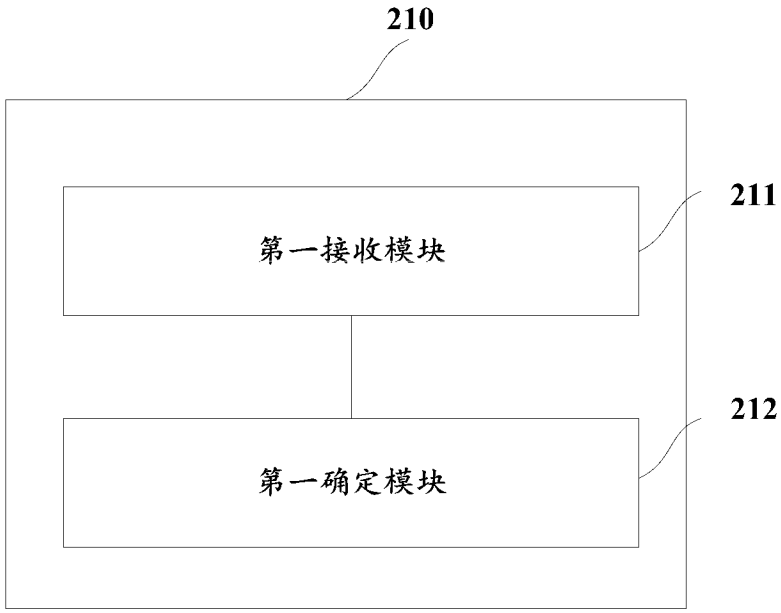

图 21

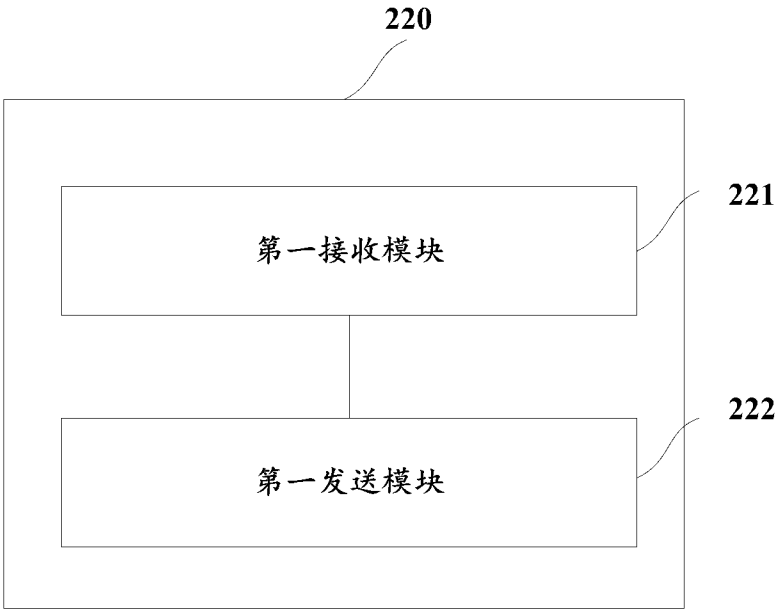

图 22

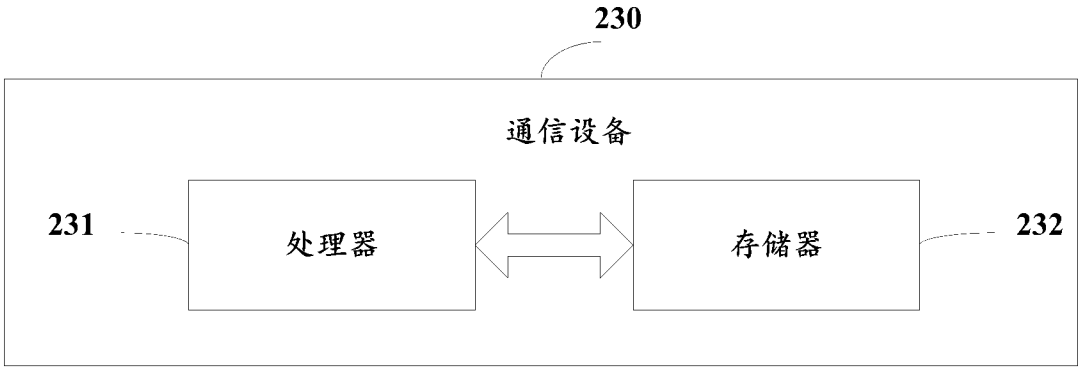

图 23

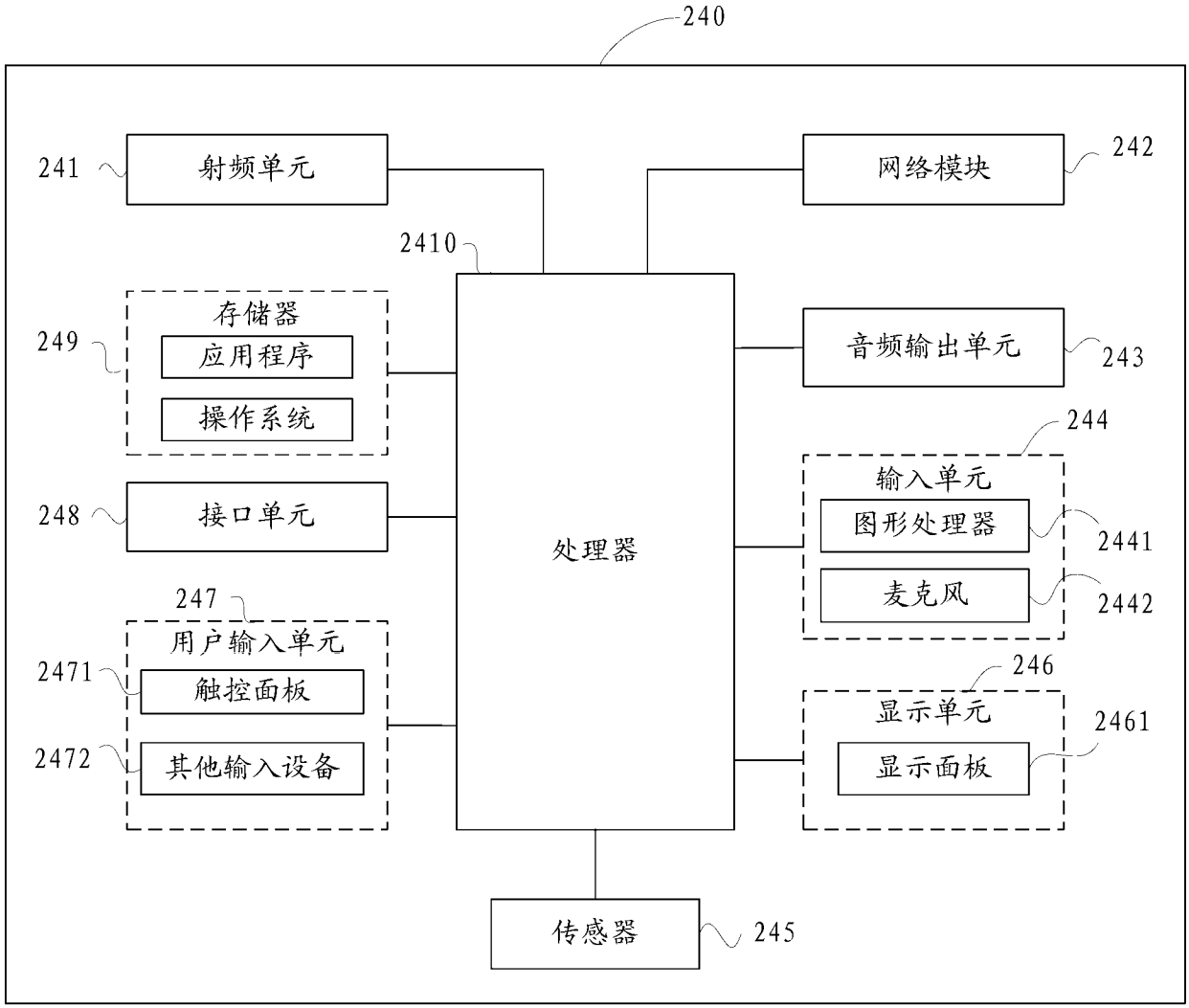
240
241
射频单元
网络模块
242
2410
存储器
249
应用程序
操作系统
音频输出单元
243
244
输入单元
248
接口单元
处理器
图形处理器
2441
麦克风
2442
247
用户输入单元
2471
触控面板
246
显示单元
2472
其他输入设备
2461
显示面板
传感器
245

图 24

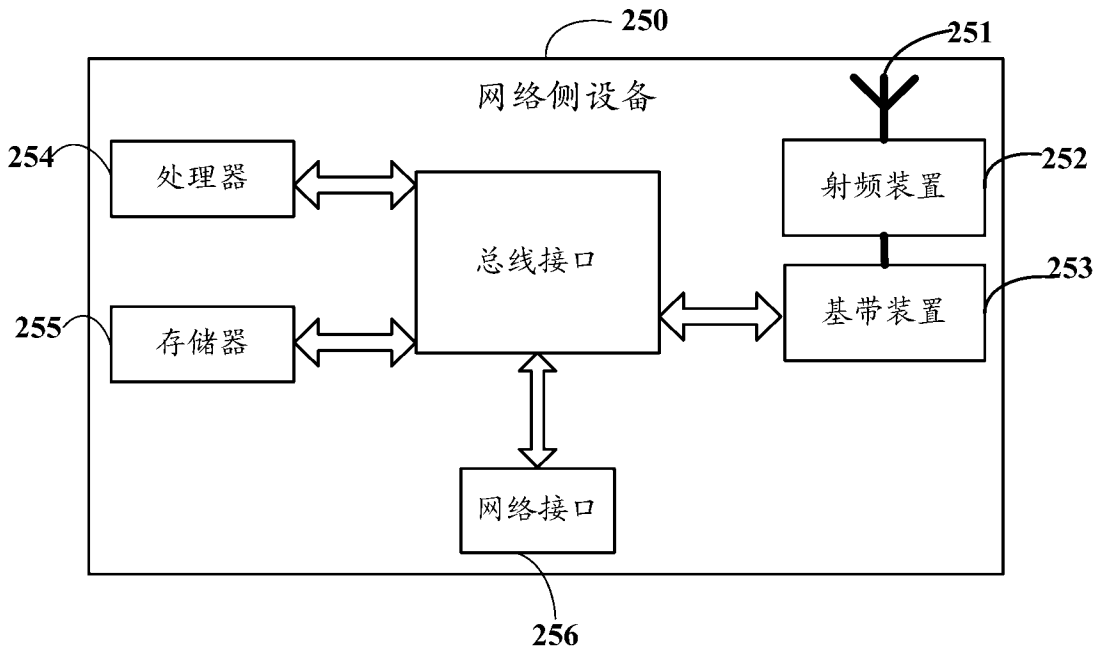
250
251
网络侧设备
254
处理器
射频装置
252
总线接口
253
255
存储器
基带装置
网络接口
256

图 25

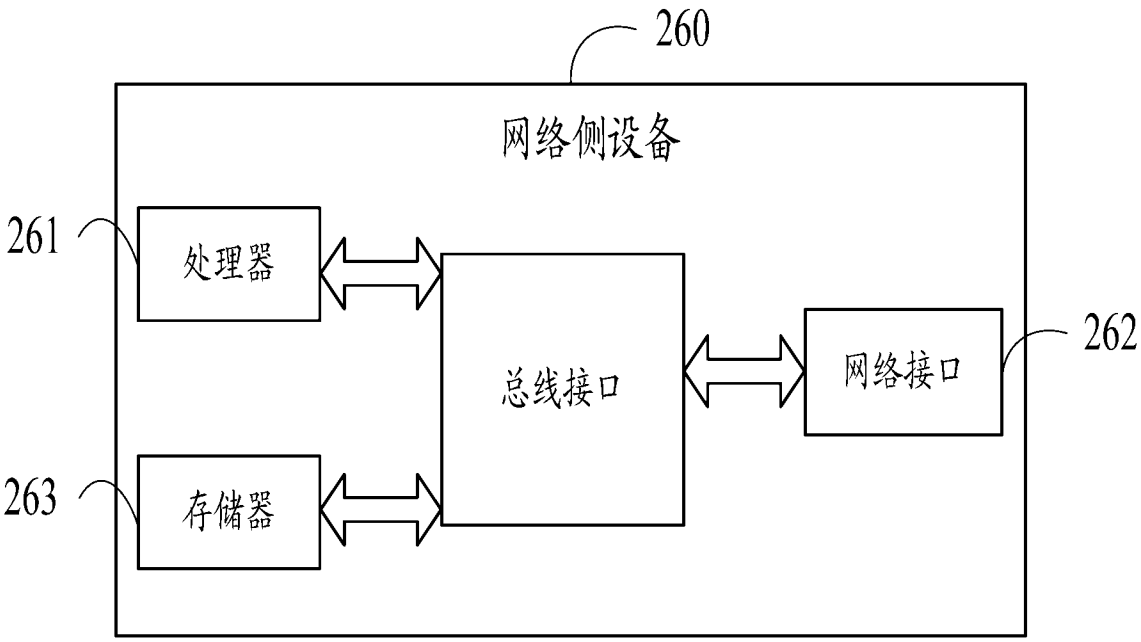

图 26

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2024/083454

A. CLASSIFICATION OF SUBJECT MATTER

H04W 12/06(2021.01)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)

IPC:H04W

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)

CNABS; CNKI; CNTXT; VEN; USTXT; WOTXT; EPTXT; 3GPP; IEEE; IETF: 环境, 物联网, 鉴权, 认证, 移动通信, 接入网, 核心网, 终端, 安全参数, 标签, ambient, IOT, A-IOT, 3GPP, access, core, UE, authenticate, security credential, tag

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 114025352 A (HUAWEI TECHNOLOGIES CO., LTD.) 08 February 2022 (2022-02-08) description, paragraphs [0172]-[0451]	1-38
A	WO 2022142446 A1 (HUAWEI TECHNOLOGIES CO., LTD.) 07 July 2022 (2022-07-07) entire document	1-38
A	NOKIA et al. "Ambient IoT Security Considerations" *3GPP TSG-RAN #99, RP-230056,* 10 March 2023 (2023-03-10), entire document	1-38

☐ 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
"D" document cited by the applicant in the international application
"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
28 June 2024	**07 July 2024**

Name and mailing address of the ISA/CN	Authorized officer
China National Intellectual Property Administration (ISA/CN) **China No. 6, Xitucheng Road, Jimenqiao, Haidian District, Beijing 100088**	Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2024/083454

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 114025352 A	08 February 2022	None	
WO 2022142446 A1	07 July 2022	None	

国际检索报告

国际申请号
PCT/CN2024/083454

A. 主题的分类

H04W 12/06(2021.01)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)

IPC:H04W

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））

CNABS;CNKI;CNTXT;VEN;USTXT;WOTXT;EPTXT;3GPP;IEEE;IETF：环境，物联网，鉴权，认证，移动通信，接入网，核心网，终端，安全参数，标签，ambient，IOT，A-IOT，3GPP，access，core，UE，authenticate，security credential，tag

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
A	CN 114025352 A (华为技术有限公司) 2022年2月8日 (2022 - 02 - 08) 说明书第[0172]-[0451]段	1-38
A	WO 2022142446 A1 (HUAWEI TECH CO LTD) 2022年7月7日 (2022 - 07 - 07) 全文	1-38
A	NOKIA 等. "Ambient IoT security considerations" 3GPP TSG-RAN #99 RP-230056, 2023年3月10日 (2023 - 03 - 10), 全文	1-38

☐ 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

“D” 申请人在国际申请中引证的文件

“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
2024年6月28日	2024年7月7日
ISA/CN的名称和邮寄地址 中国国家知识产权局 中国北京市海淀区蓟门桥西土城路6号 100088	受权官员 陈晓霞 电话号码 (+86) 0512-88996090

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2024/083454

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 114025352 A	2022年2月8日	无	
WO 2022142446 A1	2022年7月7日	无	