(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 11 月 23 日 (23.11.2023)

WIPO | PCT

(10) 国际公布号
WO 2023/221502 A1

(51) 国际专利分类号:
H04W 12/033 (2021.01)

(21) 国际申请号: PCT/CN2022/140915

(22) 国际申请日: 2022 年 12 月 22 日 (22.12.2022)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202210550259.8 2022年5月20日 (20.05.2022) CN

(71) 申请人:中国电信股份有限公司(**CHINA TELECOM CORPORATION LIMITED**) [CN/CN]; 中国北京市西城区金融大街31号, Beijing 100033 (CN)。

(72) 发明人:贾聿庸(**JIA, Yuyong**); 中国北京市西城区金融大街31号, Beijing 100033 (CN)。

(74) 代理人: 北京律智知识产权代理有限公司(**BEIJING INTELLEGAL INTELLECTUAL PROPERTY AGENT LTD.**); 中国北京市朝阳区慧忠路5号B1605、B1606、B1607, Beijing 100101 (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, 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,

WO 2023/221502 A1

(54) **Title:** DATA TRANSMISSION METHOD AND SYSTEM, AND SIGNALING SECURITY MANAGEMENT GATEWAY

(54) 发明名称: 数据传输方法和系统及信令安全管理网关

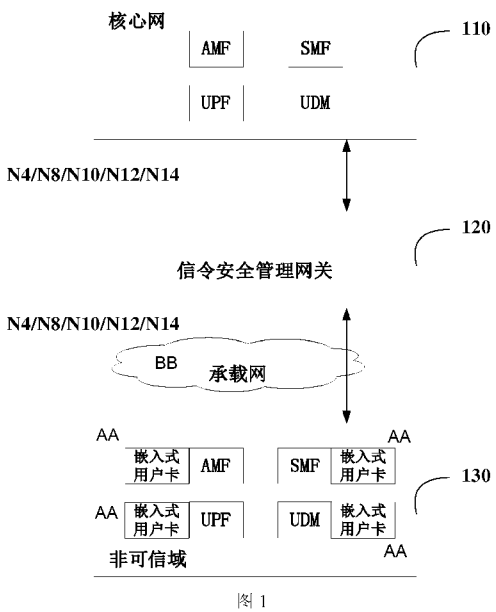

图 1

110 Core network
120 Signaling security management gateway
130 Untrusted domain
AA Embedded user card
BB Bearer network

(57) **Abstract:** The present application provides a data transmission method and system, and a signaling security management gateway, relating to the technical fields of communications and network security. The signaling security management gateway receiving a request to access a core network element by a sinking access network element, and authenticating the sinking access network element; establishing an encrypted channel between the core network element and the authenticated sinking access network element; receiving a user data synchronization request sent by the sinking access network element, and sending the user data synchronization request to the

[见续页]

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))。

corresponding core network element; receiving encrypted user data sent by the core network element, and sending the encrypted user data to the sinking access network element by means of the encrypted channel. The signaling security management gateway provides access authentication and management for the sinking access network element, and the data sent by the core network element is transmitted to the authenticated sinking access network element by means of the encrypted channel, thereby improving the security of data transmission between the core network element and the sinking access network element, and reducing the risk of information leakage.

(57) 摘要: 本申请提出一种数据传输方法和系统及信令安全管理网关，涉及通信与网络安全技术领域。信令安全管理网关接收下沉接入网元访问核心网网元的请求，对下沉接入网元进行认证；在其与认证通过的下沉接入网元之间建立加密通道；接收下沉接入网元发送的用户数据同步请求，并将用户数据同步请求发送到相应的核心网网元；接收核心网网元发送的加密用户数据，并将加密用户数据通过加密通道发送给下沉接入网元。通过信令安全管理网关为下沉接入网元提供准入认证和管理，对核心网网元发来的数据通过加密通道传输给认证通过的下沉接入网元，从而提高核心网网元与下沉接入网元之间传递数据的安全性，降低信息泄露风险。

数据传输方法和系统及信令安全管理网关

本公开基于申请号为202210550259.8、申请日为2022年5月20日、发明名称为《数据传输方法和系统及信令安全管理网关》的中国专利申请提出，并要求该中国专利申请的优先权，该中国专利申请的全部内容在此引入本公开作为参考。

技术领域

本公开涉及通信与网络安全技术领域，特别涉及一种数据传输方法和系统及信令安全管理网关。

背景技术

在第五代移动通信技术（5th Generation Mobile Communication Technology，简称5G）网络中，根据需要，核心网的一些功能会下沉到接入网。

发明内容

本公开实施例通过信令安全管理网关为下沉接入网元提供准入认证和管理，对核心网网元发来的数据通过加密通道传输给认证通过的下沉接入网元。

本公开一些实施例提出一种数据传输方法，包括：

信令安全管理网关接收下沉接入网元访问核心网网元的请求，对所述下沉接入网元进行认证；

所述信令安全管理网关在其与认证通过的所述下沉接入网元之间建立加密通道；

所述信令安全管理网关接收所述下沉接入网元发送的用户数据同步请求，并将所述用户数据同步请求发送到所述核心网网元；

所述信令安全管理网关接收所述核心网网元发送的加密用户数据，并将所述加密用户数据通过所述加密通道发送给所述下沉接入网元。

在一些实施例中，信令安全管理网关接收下沉接入网元访问核心网

网元的请求，对所述下沉接入网元进行认证包括：

信令安全管理网关接收下沉接入网元访问核心网网元的请求，所述访问核心网网元的请求携带所述下沉接入网元的标识、嵌入所述下沉接入网元的用户卡的标识以及用户签约数据中的证书信息；

所述信令安全管理网关在所述访问核心网网元的请求中的所述下沉接入网元的标识与所述用户卡的标识的绑定关系不正确或不存在的情况下，判定所述下沉接入网元认证不通过；或者，

所述信令安全管理网关在所述访问核心网网元的请求中的用户签约数据中的证书信息的时效性和合法性不满足要求的情况下，判定所述下沉接入网元认证不通过；或者，

所述信令安全管理网关在所述访问核心网网元的请求中的所述下沉接入网元的标识与所述用户卡的标识的绑定关系正确且用户签约数据中的证书信息的时效性和合法性满足要求的情况下，判定所述下沉接入网元认证通过。

在一些实施例中，所述用户数据同步请求包括所述下沉接入网元的标识和数据网络信息；所述信令安全管理网关接收所述下沉接入网元发送的用户数据同步请求，并将所述用户数据同步请求发送到所述核心网网元，包括：所述信令安全管理网关接收所述下沉接入网元发送的用户数据同步请求，并将所述用户数据同步请求发送到所述核心网网元，以使所述核心网网元根据所述下沉接入网元的标识和数据网络信息获得相应的加密用户数据。

在一些实施例中，还包括：

所述信令安全管理网关接收所述下沉接入网元发送的下载用户签约数据的请求，所述下载用户签约数据的请求包括所述下沉接入网元的标识和嵌入所述下沉接入网元的用户卡的标识和证书；

所述信令安全管理网关根据所述用户卡的标识和证书进行认证，认证通过后，查询所述下沉接入网元加载的用户签约数据，在所述下沉接入网元未加载用户签约数据或者加载的用户签约数据已过期的情况下，通知所述下沉接入网元下载新的用户签约数据，并建立所述下沉接入网元的标识与所述用户卡的标识的绑定信息。

在一些实施例中，所述信令安全管理网关通知所述下沉接入网元下载新的用户签约数据包括：

所述信令安全管理网关通知所述下沉接入网元下载新的用户签约数据，以使所述下沉接入网元通过加密通道下载新的用户签约数据并启用；

所述信令安全管理网关接收所述下沉接入网元发送的新的用户签约数据启用成功的消息。

在一些实施例中，所述信令安全管理网关为各个下沉接入网元签发用户卡，每个用户卡内包括所述用户卡的证书。

在一些实施例中，所述核心网网元包括UDM网元、UPF网元、AMF网元、SMF网元。

在一些实施例中，所述下沉接入网元包括 UDM 网元、UPF 网元、AMF网元、SMF网元。

在一些实施例中，所述用户卡包括嵌入式 UICC。

本公开一些实施例提出一种信令安全管理网关，包括：

认证模块，被配置为接收下沉接入网元访问核心网网元的请求，对所述下沉接入网元进行认证；

通道建立模块，被配置为在与所述认证模块认证通过的所述下沉接入网元之间建立加密通道；

信息代理模块，被配置为接收所述下沉接入网元发送的用户数据同步请求，并将所述用户数据同步请求发送到所述核心网网元；接收所述核心网网元发送的加密用户数据，并将所述加密用户数据通过所述加密通道发送给所述下沉接入网元。

在一些实施例中，信令安全管理网关还包括：下载管理模块，被配置为接收所述下沉接入网元发送的下载用户签约数据的请求，所述下载用户签约数据的请求包括所述下沉接入网元的标识和嵌入所述下沉接入网元的用户卡的标识和证书；根据所述用户卡的标识和证书进行认证，认证通过后，查询所述下沉接入网元加载的用户签约数据，在所述下沉接入网元未加载用户签约数据或者加载的用户签约数据已过期的情况下，通知所述下沉接入网元下载新的用户签约数据，并建立所述下沉接

入网元的标识与所述用户卡的标识的绑定信息。

在一些实施例中，所述认证模块，被配置为：

接收下沉接入网元访问核心网网元的请求，所述访问核心网网元的请求携带所述下沉接入网元的标识、嵌入所述下沉接入网元的用户卡的标识以及用户签约数据中的证书信息；

在所述访问核心网网元的请求中的所述下沉接入网元的标识与所述用户卡的标识的绑定关系不正确或不存在的情况下，判定所述下沉接入网元认证不通过；或者，

在所述访问核心网网元的请求中的用户签约数据中的证书信息的时效性和合法性不满足要求的情况下，判定所述下沉接入网元认证不通过；或者，

在所述访问核心网网元的请求中的所述下沉接入网元的标识与所述用户卡的标识的绑定关系正确且用户签约数据中的证书信息的时效性和合法性满足要求的情况下，判定所述下沉接入网元认证通过。

本公开一些实施例提出一种信令安全管理网关，包括：存储器；以及耦接至所述存储器的处理器，所述处理器被配置为基于存储在所述存储器中的指令，执行各个实施例的数据传输方法。

本公开一些实施例提出一种数据传输系统，包括：各个实施例的信令安全管理网关，核心网网元，被配置为响应用户数据同步请求，发送加密用户数据给所述信令安全管理网关，以及下沉接入网元，被配置为向所述信令安全管理网关发送访问核心网网元的请求，与所述信令安全管理网关建立加密通道，向所述信令安全管理网关发送用户数据同步请求，通过加密通道接收所述信令安全管理网关发送的加密用户数据。

本公开一些实施例提出一种非瞬时性计算机可读存储介质，其上存储有计算机程序，该程序被处理器执行时实现各个实施例的数据传输方法的步骤。

附图说明

下面将对实施例或相关技术描述中所需要使用的附图作简单地介绍。根据下面参照附图的详细描述，可以更加清楚地理解本公开。

显而易见地，下面描述中的附图仅仅是本公开的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

图 1 示出本公开一些实施例的安全数据传输系统的示意图。

图 2 示出本公开一些实施例的安全数据传输方法的示意图。

图 3 示出本公开另一些实施例的安全数据传输方法的示意图。

图 4 示出本公开一些实施例的信令安全管理网关的结构示意图。

图 5 示出本公开另一些实施例的信令安全管理网关的结构示意图。

具体实施方式

下面将结合本公开实施例中的附图，对本公开实施例中的技术方案进行清楚、完整地描述。

除非特别说明，否则，本公开中的“第一”“第二”等描述用来区分不同的对象，并不用来表示大小或时序等含义。

相关技术中核心网网元与下沉接入网元之间传递数据，存在信息泄露风险。本公开实施例通过信令安全管理网关为下沉接入网元提供准入认证和管理，对核心网网元发来的数据通过加密通道传输给认证通过的下沉接入网元，从而提高核心网网元与下沉接入网元之间传递数据的安全性，降低信息泄露风险。

图 1 示出本公开一些实施例的安全数据传输系统的示意图。

如图 1 所示，该实施例的安全数据传输系统包括：核心网网元 110，信令安全管理网关 120，以及下沉接入网元 130。

核心网网元 110 是部署在核心网的各种网元，例如可以包括通用数据管理（Unified Data Management, UDM）网元、用户面功能（UPF，User Plane Function）网元、AMF（Access and Mobility Management Function，接入和移动性管理功能）网元、SMF（Session Management Function，会话管理功能）网元等。核心网通过各种核心网网元提供终端的接入和移动性管理，认证鉴权管理，会话管理，策略控制等网络服务。以 5G 网络为例，5G SA（Stand Alone，独立组网）核心网提供 5G 终端的接入和移动性管理，认证鉴权管理，会话管理，策略控制等 5G 网络服务。

信令安全管理网关 120 可以包括：网元认证鉴权、嵌入式用户卡远程管理、信息代理等功能。其中，嵌入式用户卡远程管理功能例如可以包括：与嵌入式用户卡进行数据交互，建立加密通道；实现嵌入式用户卡数据的管理和下载，与嵌入式用户卡交互，将用户签约数据下载到嵌入式用户卡上，实现用户数据的远程配置，满足用户安全灵活地配置管理嵌入式用户卡的需要。利用嵌入式用户卡远程管理的安全能力，提供下沉接入网元的认证管理。其中，用户卡例如可以包括嵌入式通用集成电路卡（eUICC，embedded Universal Integrated Circuit Card）等。

其中，用户签约数据例如可以包括但不限于：用户鉴权相关签约数据，接入管理签约数据，会话管理签约数据等。其中，用户鉴权相关签约数据例如可以包括但不限于：国际移动用户识别码（IMSI，International Mobile Subscriber Identity），移动用户号码等，移动用户号码例如为 MSISDN（Mobile Subscriber International ISDN number，移动用户国际综合业务数字网（Integrated Services Digital Network，ISDN）号码）。接入管理签约数据例如包括但不限于：UE（User Equipment，用户设备）级别上下行带宽、禁止区域数据、业务区域限制数据、RFSP（RAT/Frequency Selection Priority，无线接入类型/频率选择优先级；RAT:Radio Access Technology，无线接入技术）、鉴权方式等。会话管理签约数据例如包括但不限于：S-NSSAI （Single Network Slice Selection Assistance Information，单个网络切片选择辅助信息）、DNN（Data Network Name，数据网络名称）、服务质量、是否默认 DNN 等。

下沉接入网元 130，是指从核心网下沉到边缘接入网的一些功能的网元。下沉接入网元 130 例如可以包括 UDM 网元、UPF 网元、AMF 网元、SMF 网元等。例如，下沉 UDM 网元可以是核心网的 UDM 网元的部分功能下沉到边缘接入网形成的网元。下沉接入网元 130 可以与核心网网元 110 进行用户鉴权等数据交互。

下沉接入网元 130 可设置嵌入式用户卡。嵌入式用户卡可存储卡文件、数据和应用等，可远程下载用户签约数据。用户签约数据例如可以包括但不限于：用户识别信息和业务信息等。嵌入式用户卡例如可以包括嵌入式 UICC 等。

核心网网元 110 与信令安全管理网关 120 之间的接口例如可以包括 N4/N8/N10/N12/N14 等，信令安全管理网关 120 与下沉接入网元 130 之间的接口例如可以包括 N4/N8/N10/N12/N14 等。

为了实现安全数据传输，在数据传输系统中，信令安全管理网关 120，可被配置为接收下沉接入网元访问核心网网元的请求，对下沉接入网元进行认证；与认证通过的下沉接入网元建立加密通道；接收下沉接入网元发送的用户数据同步请求，将用户数据同步请求发送到相应的核心网网元；接收核心网网元发送的加密用户数据，将加密用户数据通过加密通道发送给下沉接入网元；核心网网元 110，可被配置为响应用户数据同步请求，发送加密用户数据给信令安全管理网关；以及下沉接入网元 130，可被配置为向信令安全管理网关发送访问核心网网元的请求，与信令安全管理网关建立加密通道，向信令安全管理网关发送用户数据同步请求，通过加密通道接收信令安全管理网关发送的加密用户数据。

为了安全下载用户签约数据，在数据传输系统中，信令安全管理网关 120，可被配置为接收下沉接入网元发送的下载用户签约数据的请求，该请求可包括下沉接入网元的标识和嵌入下沉接入网元的用户卡的标识和证书；根据用户卡的标识和证书进行认证，认证通过后，查询下沉接入网元加载的用户签约数据，在下沉接入网元未加载用户签约数据或者加载的用户签约数据已过期的情况下，通知下沉接入网元下载新的用户签约数据，建立下沉接入网元的标识和嵌入下沉接入网元的用户卡的标识的绑定信息。

图 2 示出本公开一些实施例的安全数据传输方法的示意图。

如图 2 所示，该实施例的安全数据传输方法可以包括以下步骤。

在步骤 200，信令安全管理网关为各个下沉接入网元签发用户卡，每个用户卡内包括签发的用户卡的证书。

在步骤 210，信令安全管理网关接收到下沉接入网元发送的下载用户签约数据的请求，请求包括下沉接入网元的标识和嵌入下沉接入网元的用户卡的标识和证书。

在步骤 220，信令安全管理网关根据用户卡的标识和证书进行认证，认证通过后，查询下沉接入网元加载的用户签约数据，在下沉接入网元

未加载用户签约数据或者加载的用户签约数据已过期的情况下，通知下沉接入网元下载新的用户签约数据，建立下沉接入网元的标识和嵌入下沉接入网元的用户卡的标识的绑定信息，在下沉接入网元加载的用户签约数据未过期的情况下，通知下沉接入网元无需下载或者停止下载用户签约数据。

其中，根据用户卡的标识和证书进行认证包括：如果用户卡的证书的颁发者是信令安全管理网关，且用户卡的证书在有效期内，且用户卡的证书与用户卡的标识是匹配的，认证通过，否则，认证不通过。

在步骤230，信令安全管理网关通知下沉接入网元下载新的用户签约数据。

在步骤240，下沉接入网元通过加密通道下载新的用户签约数据并启用，旧的用户签约数据可以删除。

在步骤250，信令安全管理网关接收下沉接入网元发送的新的用户签约数据启用成功的消息。

在步骤260，信令安全管理网关接收下沉接入网元访问核心网网元的请求，其中携带下沉接入网元的标识、嵌入下沉接入网元的用户卡的标识以及用户签约数据中的证书信息。

在步骤270，信令安全管理网关对下沉接入网元进行认证，例如可以包括：

在该访问请求中的下沉接入网元的标识与用户卡的标识的绑定关系不正确或不存在的情况下，判定下沉接入网元认证不通过；或者，

在该访问请求中的用户签约数据中的证书信息的时效性和合法性不满足要求的情况下，判定下沉接入网元认证不通过；或者，

在该访问请求中的下沉接入网元的标识与用户卡的标识的绑定关系正确且用户签约数据中的证书信息的时效性和合法性满足要求的情况下，判定下沉接入网元认证通过。

认证通过后，才允许执行步骤290~2150。

在步骤 280，信令安全管理网关发送认证结果给下沉接入网元。其中，认证结果例如包括认证通过或认证不通过。

在步骤290，信令安全管理网关与认证通过的下沉接入网元建立加密

通道。

加密通道的建立方法可以参考现有技术。加密通道例如包括通信双方协商的加密密钥信息。加密通道建立后，通信双方可以利用协商的加密密钥传输信息。第三方由于不知道加密密钥，即使截获加密信息，也无从获知传输的信息。

在步骤 2100，信令安全管理网关接收下沉接入网元发送的用户数据同步请求，该用户数据同步请求可以包括下沉接入网元的标识和数据网络信息。

其中，数据网络信息例如包括但不限于数据网络名称（Data Network name，DNN）。

在步骤 2110，信令安全管理网关将用户数据同步请求发送到相应的核心网网元。

例如，信令安全管理网关将下沉 UDM 网元的用户数据同步请求转发到核心网 UDM 网元。

核心网网元对于下沉接入网元来说是隐藏的，下沉接入网元将请求发送到信令安全管理网关，无需发送核心网网元，信令安全管理网关可将请求发送到核心网网元。

在步骤 2120，核心网网元查找下沉接入网元的标识和数据网络信息相应的用户数据并加密得到加密用户数据。

其中，核心网网元可按照与下沉接入网元预先协商好的密钥，对用户数据加密得到加密用户数据。

其中，用户数据例如是用户卡和鉴权数据等，例如，IMSI、KI（Key identifier，密钥标识）等。

在步骤 2130，信令安全管理网关接收核心网网元发送的加密用户数据。

在步骤 2140，信令安全管理网关将加密用户数据通过加密通道发送给下沉接入网元。

在步骤 2150，下沉接入网元接收加密用户数据，解密得到用户数据，根据业务需要使用用户数据进行业务保障，例如保障业务不中断。

其中，下沉接入网元可按照与核心网网元预先协商好的密钥，对加

密用户数据解密得到用户数据。

上述实施例通过信令安全管理网关为下沉接入网元提供准入认证和管理，对核心网网元发来的数据通过加密通道传输给认证通过的下沉接入网元，从而提高核心网网元与下沉接入网元之间传递数据的安全性，降低信息泄露风险。

下面结合图 3 描述核心网 UDM 网元与下沉 UDM 网元通过信令安全管理网关安全传输用户数据的方法。

图 3 示出本公开另一些实施例的安全数据传输方法的示意图。

如图 3 所示，该实施例的安全数据传输方法可以包括以下步骤。

在步骤 300，下沉 UDM 网元具备嵌入式 UICC，且该 UICC 是由信令安全管理网关签发。

在步骤 310，下沉 UDM 网元按时或按需请求接入 5G SA 网络，通过嵌入式 UICC 主动连接信令安全管理网关，请求下载用户签约数据（设为 Profile），请求中携带嵌入式 UICC 的 EID（Electronic Identity，电子身份标识）和下沉 UDM 网元的设备 ID。

在步骤 320，网元接入管理网关收到请求后，根据 EID 及 UICC 内证书信息进行安全认证，认证通过后，查询设备 ID 相应的下沉 UDM 网元是否已加载 Profile；若未加载或 Profile 已过期，则通知该下沉 UDM 网元准备进行用户签约数据下载，并将 EID 和设备 ID 进行绑定；若已加载 Profile 且 Profile 未过期，则通知下沉 UDM 网元停止下载。

其中，根据 EID 及 UICC 内证书信息进行安全认证包括：如果 UICC 内证书的颁发者是信令安全管理网关，且 UICC 内证书在有效期内，且 UICC 内证书与 EID 是匹配的，认证通过，否则，认证不通过。

在步骤 330，信令安全管理网关发送请求到下沉 UDM 网元，要求建立加密通道、下载并启用 Profile。

在步骤 340，下沉 UDM 网元与信令安全管理网关间建立加密通道，通过加密通道下载新的 Profile，若之前已加载过期 Profile，则删除旧 Profile，启用新的 Profile。

在步骤 350，下沉 UDM 网元向信令安全管理网关返回 Profile 启用成功的消息。

在步骤360，下沉UDM网元发起访问5G SA网络中的核心网UDM网元的请求到信令安全管理网关，携带嵌入式UICC的EID，设备ID和Profile内的证书信息。

在步骤370，信令安全管理网关依据下沉UDM网元的请求信息，检查EID和设备ID绑定关系是否正确，若不正确或不存在，则不允许下沉UDM网元接入；若正确，则认证Profile内证书的时效性和合法性，认证通过后，允许下沉UDM网元接入。

在步骤380，认证通过后，信令安全管理网关发送认证通过的通知给下沉UDM网元。

在步骤390，下沉UDM网元利用嵌入式UICC相关安全信息，如EID，与信令安全管理网关建立加密通道。

在步骤3100，下沉UDM网元发送用户数据同步请求至信令安全管理网关，携带DNN、设备ID等信息。

在步骤3110，信令安全管理网关隐藏核心网UDM拓扑信息，将用户数据同步请求转发至相应的核心网UDM网元请求同步用户数据。

在步骤3120，核心网UDM网元接到用户数据同步请求后，根据设备ID及DNN等信息，查找到相关的用户卡数据和鉴权数据等用户数据，如IMSI、KI等数据，并对用户数据进行加密处理，加密密钥由核心网UDM网元与下沉UDM网元预先协商或预先设置。

在步骤3130，核心网UDM网元将加密用户数据传递至信令安全管理网关。

在步骤3140，信令安全管理网关将加密用户数据通过加密通道传递到下沉UDM网元。

在步骤3150，下沉UDM网元解密加密用户数据得到用户数据，依据5G应用场景（如应急通信、紧急通信等）的需求，按需使用用户卡数据及鉴权数据等用户数据，保障5G业务不中断。

上述实施例，不改变现有5G的架构和业务实现流程，利用嵌入式UICC远程配置技术和安全加密技术，对5G下沉UDM等不可信接入网元设备接入5G核心网进行安全认证和管理，有效降低下沉网元对5G核心网的安全交互风险，同时，对请求的5G核心网UDM中的敏感数据（如

用户卡数据和鉴权数据）进行数据加密和通道加密传递，有效降低信息泄露安全风险，从而提高 5G 的网络安全和数据安全。

图 4 示出本公开一些实施例的信令安全管理网关的结构示意图。

如图 4 所示，该实施例的信令安全管理网关 120 可以包括：

认证模块 410，被配置为接收下沉接入网元访问核心网网元的请求，对下沉接入网元进行认证；

通道建立模块 420，被配置为与认证通过的下沉接入网元建立加密通道；

信息代理模块 430，被配置为接收下沉接入网元发送的用户数据同步请求，将用户数据同步请求发送到相应的核心网网元；接收核心网网元发送的加密用户数据，将加密用户数据通过加密通道发送给下沉接入网元。

在一些实施例中，信令安全管理网关 120 还包括：下载管理模块 440，被配置为接收到下沉接入网元发送的下载用户签约数据的请求，请求包括下沉接入网元的标识和嵌入下沉接入网元的用户卡的标识和证书；根据用户卡的标识和证书进行认证，认证通过后，查询下沉接入网元加载的用户签约数据，在下沉接入网元未加载用户签约数据或者加载的用户签约数据已过期的情况下，通知下沉接入网元下载新的用户签约数据，建立下沉接入网元的标识和嵌入下沉接入网元的用户卡的标识的绑定信息。

在一些实施例中，认证模块 410，还被配置为：

接收下沉接入网元访问核心网网元的请求，其中携带下沉接入网元的标识、嵌入下沉接入网元的用户卡的标识以及用户签约数据中的证书信息；

在访问请求的下沉接入网元的标识与用户卡的标识的绑定关系不正确或不存在的情况下，判定下沉接入网元认证不通过；或者，

在访问请求的用户签约数据中的证书信息的时效性和合法性不满足要求的情况下，判定下沉接入网元认证不通过；或者，

在访问请求的下沉接入网元的标识与用户卡的标识的绑定关系正确且用户签约数据中的证书信息的时效性和合法性满足要求的情况下，判

定下沉接入网元认证通过。

图 5 示出本公开另一些实施例的信令安全管理网关的结构示意图。

如图 5 所示，该实施例的信令安全管理网关 120 包括：存储器 510 以及耦接至该存储器 510 的处理器 520，处理器 520 被配置为基于存储在存储器 510 中的指令，执行前述任意一些实施例中的安全数据传输方法。

其中，存储器 510 例如可以包括系统存储器、固定非易失性存储介质等。系统存储器例如存储有操作系统、应用程序、引导装载程序（Boot Loader）以及其他程序等。

其中，处理器 520 可以用通用处理器、数字信号处理器（Digital Signal Processor，DSP）、应用专用集成电路（Application Specific Integrated Circuit，ASIC）、现场可编程门阵列（Field Programmable Gate Array ，FPGA）或其它可编程逻辑设备、分立门或晶体管等分立硬件组件方式来实现。

信令安全管理网关 120 还可以包括输入输出接口 530、网络接口 540、存储接口 550 等。这些接口 530，540，550 以及存储器 510 和处理器 520 之间例如可以通过总线 560 连接。其中，输入输出接口 530 为显示器、鼠标、键盘、触摸屏等输入输出设备提供连接接口。网络接口 540 为各种联网设备提供连接接口。存储接口 550 为 SD 卡、U 盘等外置存储设备提供连接接口。总线 560 可以使用多种总线结构中的任意总线结构。例如，总线结构包括但不限于工业标准体系结构（Industry Standard Architecture，ISA）总线、微通道体系结构（Micro Channel Architecture，MCA）总线、外围组件互连（Peripheral Component Interconnect ，PCI）总线。

本领域内的技术人员应当明白，本公开的实施例可提供为方法、系统、或计算机程序产品。因此，本公开可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本公开可采用在一个或多个其中包含有计算机程序代码的非瞬时性计算机可读存储介质（包括但不限于磁盘存储器、CD-ROM、光学存储器等）上实施的计算机程序产品的形式。

本公开是参照根据本公开实施例的方法、设备（系统）、和计算机程

序产品的流程图和／或方框图来描述的。应理解为可由计算机程序指令实现流程图和／或方框图中的每一流程和／或方框、以及流程图和／或方框图中的流程和／或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和／或方框图一个方框或多个方框中指定的功能的装置。

这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和／或方框图一个方框或多个方框中指定的功能。

这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和／或方框图一个方框或多个方框中指定的功能的步骤。

以上所述仅为本公开的较佳实施例，并不用以限制本公开，凡在本公开的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本公开的保护范围之内。

权利要求

1. 一种数据传输方法，其中，包括：

信令安全管理网关接收下沉接入网元访问核心网网元的请求，对所述下沉接入网元进行认证；

所述信令安全管理网关在其与认证通过的所述下沉接入网元之间建立加密通道；

所述信令安全管理网关接收所述下沉接入网元发送的用户数据同步请求，并将所述用户数据同步请求发送到所述核心网网元；

所述信令安全管理网关接收所述核心网网元发送的加密用户数据，并将所述加密用户数据通过所述加密通道发送给所述下沉接入网元。

2. 根据权利要求 1 所述的方法，其中，信令安全管理网关接收下沉接入网元访问核心网网元的请求，对所述下沉接入网元进行认证包括：

信令安全管理网关接收下沉接入网元访问核心网网元的请求，所述访问核心网网元的请求携带所述下沉接入网元的标识、嵌入所述下沉接入网元的用户卡的标识以及用户签约数据中的证书信息；

所述信令安全管理网关在所述访问核心网网元的请求中的所述下沉接入网元的标识与所述用户卡的标识的绑定关系不正确或不存在的情况下，判定所述下沉接入网元认证不通过；或者，

所述信令安全管理网关在所述访问核心网网元的请求中的用户签约数据中的证书信息的时效性和合法性不满足要求的情况下，判定所述下沉接入网元认证不通过；或者，

所述信令安全管理网关在所述访问核心网网元的请求中的所述下沉接入网元的标识与所述用户卡的标识的绑定关系正确且用户签约数据中的证书信息的时效性和合法性满足要求的情况下，判定所述下沉接入网元认证通过。

3. 根据权利要求 1 所述的方法，其中，所述用户数据同步请求包括所述下沉接入网元的标识和数据网络信息；

所述信令安全管理网关接收所述下沉接入网元发送的用户数据同步

请求，并将所述用户数据同步请求发送到所述核心网网元，包括：

所述信令安全管理网关接收所述下沉接入网元发送的用户数据同步请求，并将所述用户数据同步请求发送到所述核心网网元，以使所述核心网网元根据所述下沉接入网元的标识和数据网络信息获得相应的加密用户数据。

4. 根据权利要求 1 所述的方法，其中，还包括：

所述信令安全管理网关接收所述下沉接入网元发送的下载用户签约数据的请求，所述下载用户签约数据的请求包括所述下沉接入网元的标识和嵌入所述下沉接入网元的用户卡的标识和证书；

所述信令安全管理网关根据所述用户卡的标识和证书进行认证，认证通过后，查询所述下沉接入网元加载的用户签约数据，在所述下沉接入网元未加载用户签约数据或者加载的用户签约数据已过期的情况下，通知所述下沉接入网元下载新的用户签约数据，并建立所述下沉接入网元的标识与所述用户卡的标识的绑定信息。

5. 根据权利要求 4 所述的方法，其中，所述信令安全管理网关通知所述下沉接入网元下载新的用户签约数据包括：

所述信令安全管理网关通知所述下沉接入网元下载新的用户签约数据，以使所述下沉接入网元通过加密通道下载新的用户签约数据并启用；

所述信令安全管理网关接收所述下沉接入网元发送的新的用户签约数据启用成功的消息。

6. 根据权利要求 1 所述的方法，其中，

所述信令安全管理网关为各个下沉接入网元签发用户卡，每个用户卡内包括所述用户卡的证书。

7. 根据权利要求 2-6 任一项所述的方法，其中，

所述核心网网元包括 UDM 网元、UPF 网元、AMF 网元、SMF 网

元；

所述下沉接入网元包括 UDM 网元、UPF 网元、AMF 网元、SMF 网元；

所述用户卡包括嵌入式 UICC。

8. 一种信令安全管理网关，其中，包括：

认证模块，被配置为接收下沉接入网元访问核心网网元的请求，对所述下沉接入网元进行认证；

通道建立模块，被配置为在与所述认证模块认证通过的所述下沉接入网元之间建立加密通道；

信息代理模块，被配置为接收所述下沉接入网元发送的用户数据同步请求，并将所述用户数据同步请求发送到所述核心网网元；接收所述核心网网元发送的加密用户数据，并将所述加密用户数据通过所述加密通道发送给所述下沉接入网元。

9. 根据权利要求 8 所述的信令安全管理网关，其中，还包括：

下载管理模块，被配置为接收所述下沉接入网元发送的下载用户签约数据的请求，所述下载用户签约数据的请求包括所述下沉接入网元的标识和嵌入所述下沉接入网元的用户卡的标识和证书；根据所述用户卡的标识和证书进行认证，认证通过后，查询所述下沉接入网元加载的用户签约数据，在所述下沉接入网元未加载用户签约数据或者加载的用户签约数据已过期的情况下，通知所述下沉接入网元下载新的用户签约数据，并建立所述下沉接入网元的标识与所述用户卡的标识的绑定信息。

10. 根据权利要求 8 所述的信令安全管理网关，其中，所述认证模块，被配置为：

接收下沉接入网元访问核心网网元的请求，所述访问核心网网元的请求携带所述下沉接入网元的标识、嵌入所述下沉接入网元的用户卡的标识以及用户签约数据中的证书信息；

在所述访问核心网网元的请求中的所述下沉接入网元的标识与所述

用户卡的标识的绑定关系不正确或不存在的情况下，判定所述下沉接入网元认证不通过；或者，

在所述访问核心网网元的请求中的用户签约数据中的证书信息的时效性和合法性不满足要求的情况下，判定所述下沉接入网元认证不通过；或者，

在所述访问核心网网元的请求中的所述下沉接入网元的标识与所述用户卡的标识的绑定关系正确且用户签约数据中的证书信息的时效性和合法性满足要求的情况下，判定所述下沉接入网元认证通过。

11. 一种信令安全管理网关，包括：

存储器；以及

耦接至所述存储器的处理器，所述处理器被配置为基于存储在所述存储器中的指令，执行权利要求 1-7 中任一项所述的数据传输方法。

12. 一种数据传输系统，包括：

权利要求 8-11 任一项所述的信令安全管理网关，

核心网网元，被配置为响应用户数据同步请求，发送加密用户数据给所述信令安全管理网关，

以及

下沉接入网元，被配置为向所述信令安全管理网关发送访问核心网网元的请求，与所述信令安全管理网关建立加密通道，向所述信令安全管理网关发送用户数据同步请求，通过加密通道接收所述信令安全管理网关发送的加密用户数据。

13. 根据权利要求 12 所述的数据传输系统，其中，

所述核心网网元包括 UDM 网元、UPF 网元、AMF 网元、SMF 网元；

所述下沉接入网元包括 UDM 网元、UPF 网元、AMF 网元、SMF 网元。

14. 一种非瞬时性计算机可读存储介质，其上存储有计算机程序，该程序被处理器执行时实现权利要求 1-7 中任一项所述的数据传输方法的步骤。

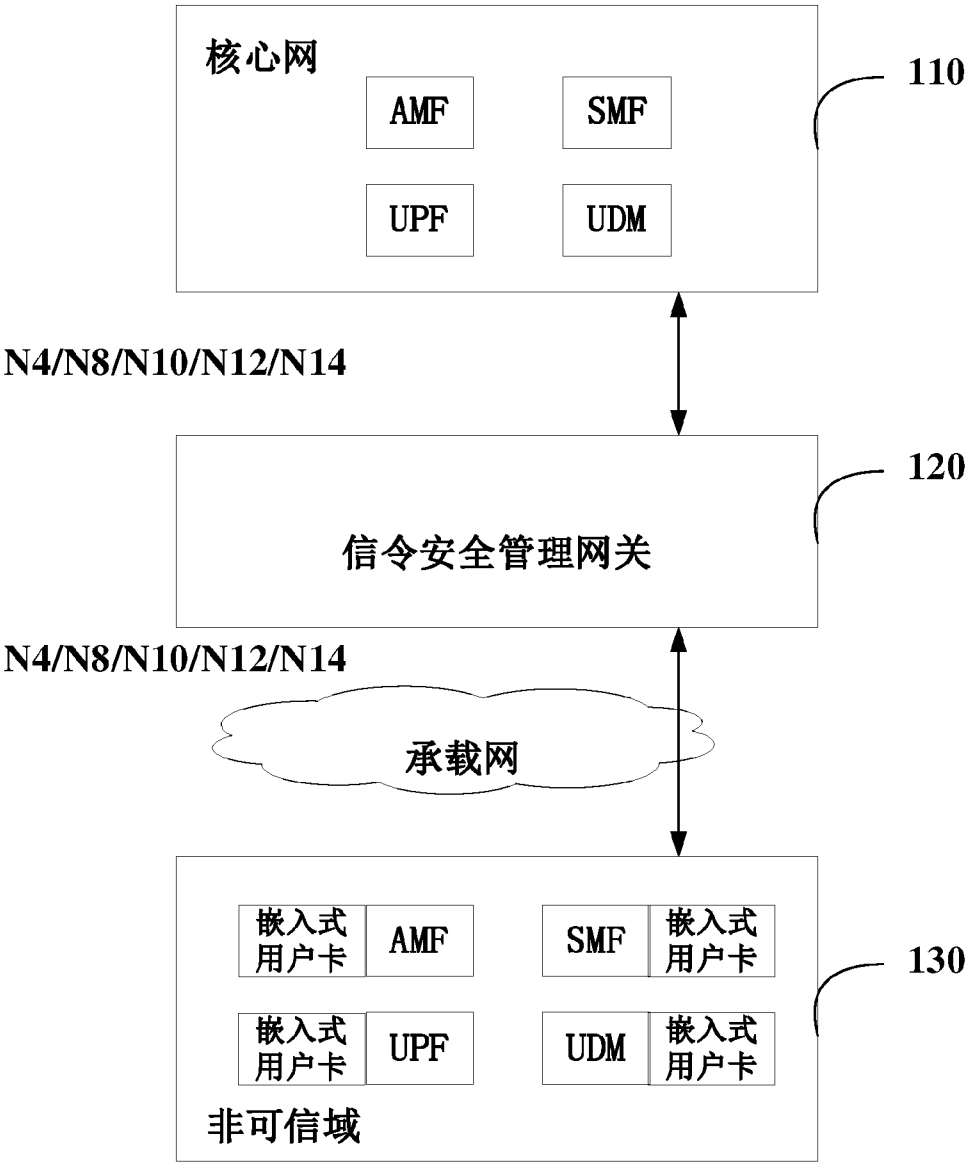
核心网
AMF
SMF
UPF
UDM
110
N4/N8/N10/N12/N14
信令安全管理网关
120
N4/N8/N10/N12/N14
承载网
嵌入式用户卡
AMF
SMF
嵌入式用户卡
嵌入式用户卡
UPF
UDM
嵌入式用户卡
130
非可信域

图 1

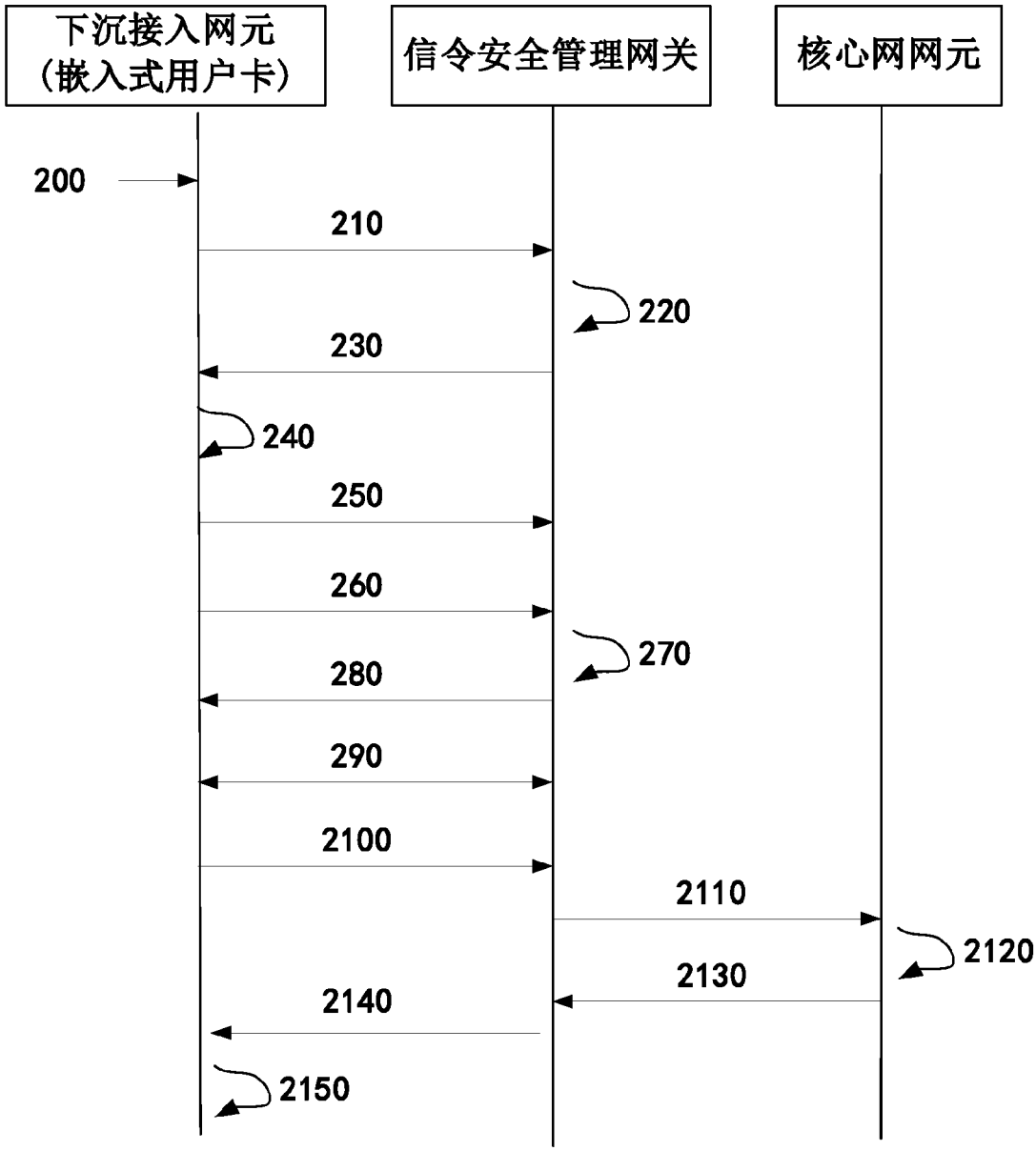
下沉接入网元
（嵌入式用户卡）
信令安全管理网关
核心网网元
200
210
220
230
240
250
260
270
280
290
2100
2110
2120
2130
2140
2150

图 2

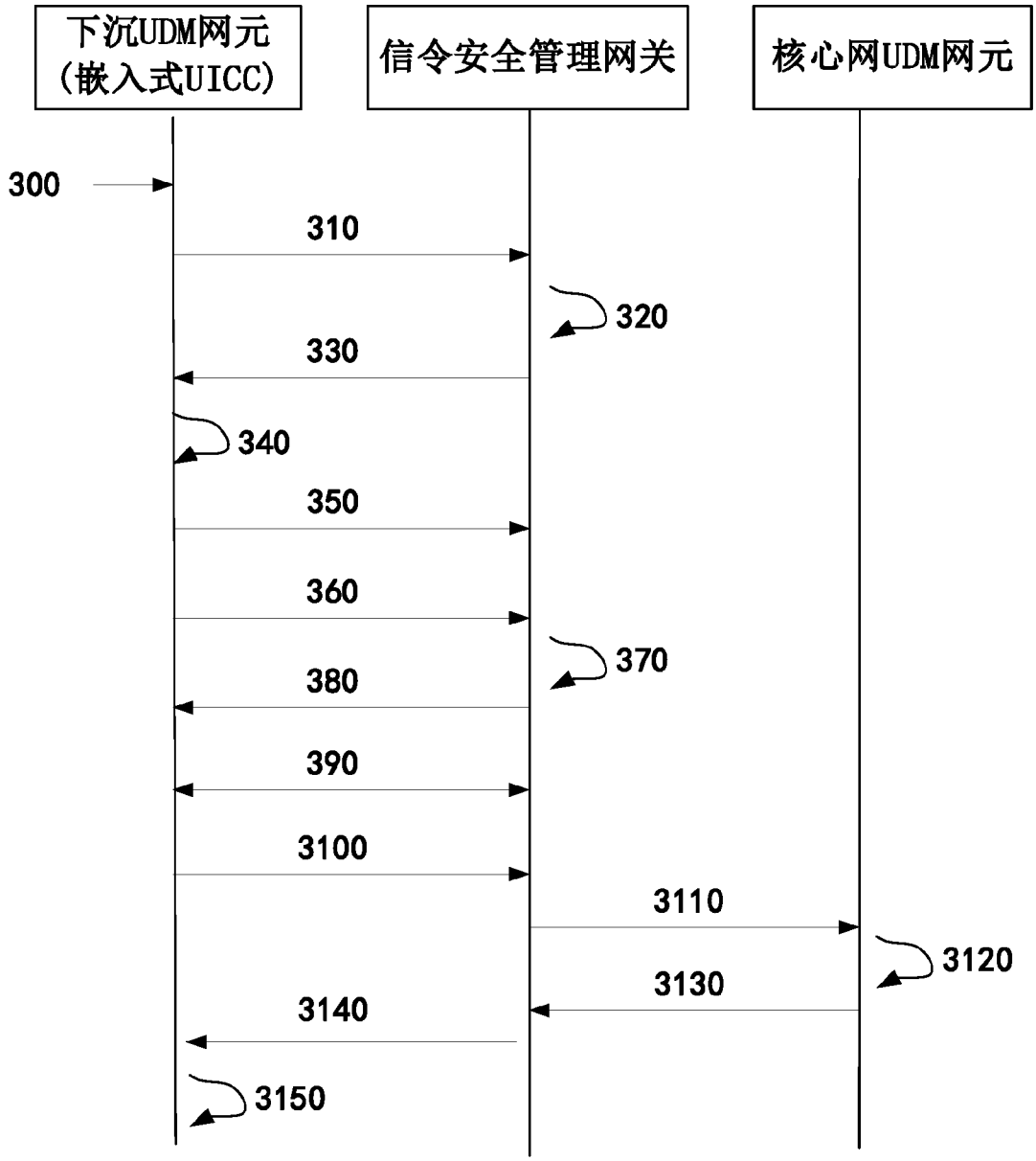
下沉UDM网元
(嵌入式UICC)
信令安全管理网关
核心网UDM网元
300
310
320
330
340
350
360
370
380
390
3100
3110
3120
3130
3140
3150

图 3

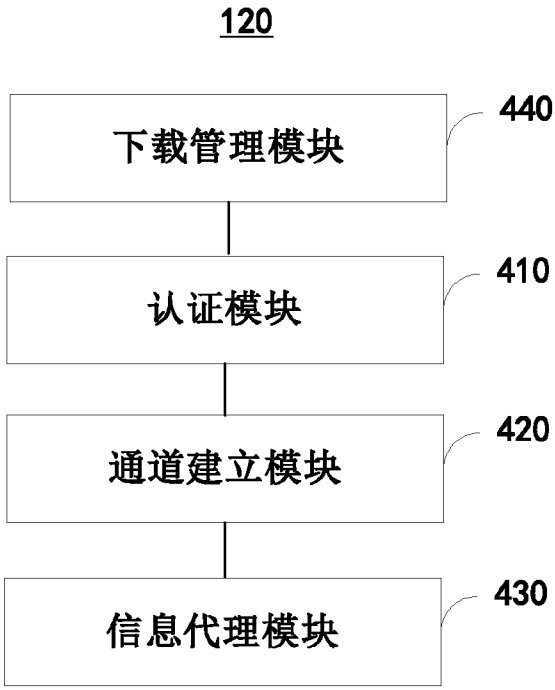

图 4

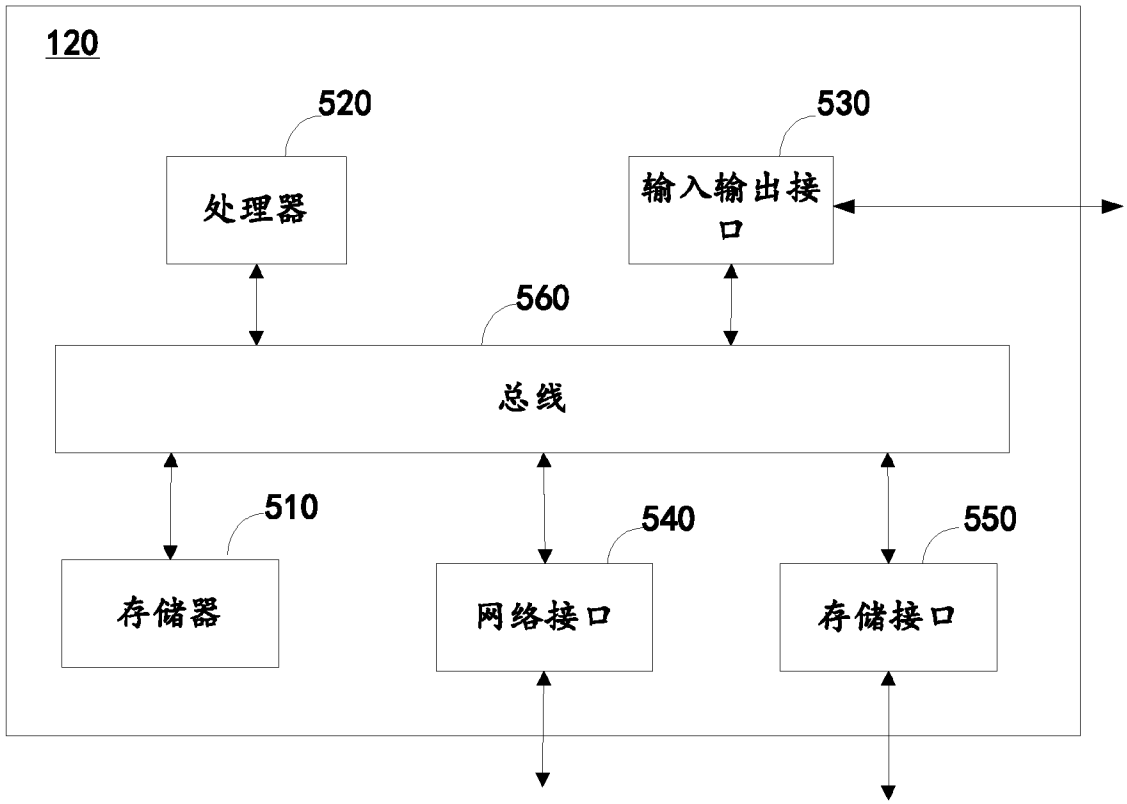

图 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2022/140915

A. CLASSIFICATION OF SUBJECT MATTER

H04W 12/033(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)

H04W; H04Q

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; IEEE: 核心网, 骨干网, core network, 接入网, RAN, 5G, NR, 下沉, sink+, 网关, gateway, GW, 认证, authenticat+, 请求, request, 加密, encrypt+, 隧道, tunnel, 用户数据, user data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 113068175 A (CHINA TELECOM CORP., LTD.) 02 July 2021 (2021-07-02) description, paragraphs 32-60	1-14
A	CN 113747515 A (HUAWEI TECHNOLOGIES CO., LTD.) 03 December 2021 (2021-12-03) entire document	1-14
A	CN 111147426 A (ZTE CORP.) 12 May 2020 (2020-05-12) entire document	1-14
A	CN 112422679 A (CHINA UNITED NETWORK COMMUNICATIONS GROUP CO., LTD.) 26 February 2021 (2021-02-26) entire document	1-14
A	WO 2021244509 A1 (ZTE CORP.) 09 December 2021 (2021-12-09) entire document	1-14

☐ 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
16 January 2023	**28 January 2023**

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

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2022/140915

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 113068175 A	02 July 2021	None	
CN 113747515 A	03 December 2021	WO 2021238383 A1	02 December 2021
CN 111147426 A	12 May 2020	WO 2020093994 A1	14 May 2020
		US 2022030438 A1	27 January 2022
		EP 3879779 A1	15 September 2021
CN 112422679 A	26 February 2021	None	
WO 2021244509 A1	09 December 2021	CN 112788594 A	11 May 2021

国际检索报告

国际申请号
PCT/CN2022/140915

A. 主题的分类

H04W 12/033(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)

H04W; H04Q

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;IEEE:核心网，骨干网，core network，接入网，RAN，5G，NR，下沉，sink+，网关，gateway，GW，认证，authenticat+，请求，request，加密，encrypt+，隧道，tunnel，用户数据，user data

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 113068175 A (中国电信股份有限公司) 2021年7月2日 (2021-07-02) 说明书第32-60段	1-14
A	CN 113747515 A (华为技术有限公司) 2021年12月3日 (2021-12-03) 全文	1-14
A	CN 111147426 A (中兴通讯股份有限公司) 2020年5月12日 (2020-05-12) 全文	1-14
A	CN 112422679 A (中国联合网络通信集团有限公司) 2021年2月26日 (2021-02-26) 全文	1-14
A	WO 2021244509 A1 (ZTE CORPORATION) 2021年12月9日 (2021-12-09) 全文	1-14

☐ 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
2023年1月16日	2023年1月28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 颜悦 电话号码 86-(10)-53961643

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2022/140915

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	113068175	A	2021年7月2日	无			
CN	113747515	A	2021年12月3日	WO	2021238383	A1	2021年12月2日
CN	111147426	A	2020年5月12日	WO	2020093994	A1	2020年5月14日
				US	2022030438	A1	2022年1月27日
				EP	3879779	A1	2021年9月15日
CN	112422679	A	2021年2月26日	无			
WO	2021244509	A1	2021年12月9日	CN	112788594	A	2021年5月11日