(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 7 月 11 日 (11.07.2024)

WIPO | PCT

(10) 国际公布号
WO 2024/146582 A1

(51) 国际专利分类号:
*H04W 12/06* (2021.01)

(21) 国际申请号: PCT/CN2024/070490

(22) 国际申请日: 2024 年 1 月 4 日 (04.01.2024)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202310021264.4 2023年1月6日 (06.01.2023) CN

(71) 申请人: 华 为 技 术 有 限 公 司 **(HUAWEI TECHNOLOGIES CO., LTD.)** [CN/CN]; 中 国 广 东 省 深 圳 市 龙 岗 区 坂 田 华 为 总 部 办 公 楼, Guangdong 518129 (CN)。

(72) 发明人: 吴 义 壮 **(WU, Yizhuang)**; 中 国 广 东 省 深 圳 市 龙 岗 区 坂 田 华 为 总 部 办 公 楼, Guangdong 518129 (CN)。

(74) 代理人: 北 京 龙 双 利 达 知 识 产 权 代 理 有 限 公 司 **(LONGSUN LEAD IP LTD.)**; 中 国 北 京 市 海 淀 区 北 清 路 81 号 院 二 区 3 号 楼 8 层 801-1 室, Beijing 100094 (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, MU, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA,

WO 2024/146582 A1

(54) **Title:** COMMUNICATION METHOD AND COMMUNICATION APPARATUS

(54) 发明名称: 通信方法和通信装置

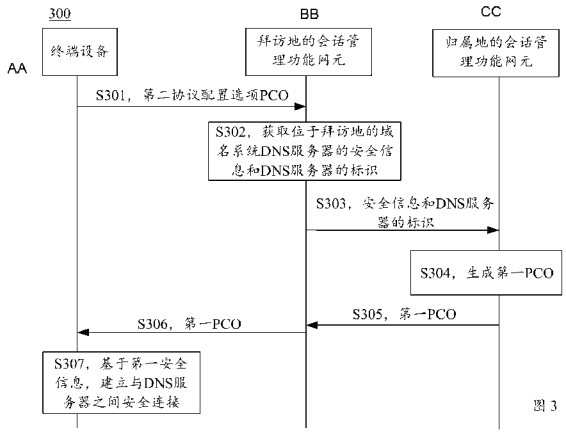



图 3

| | |
|---|---|
| S301 | Second protocol configuration option (PCO) |
| S302 | Acquire security information of a visited domain name system (DNS) server and an identifier of the DNS server |
| S303 | The security information and the identifier of the DNS server |
| S304 | Generate a first PCO |
| S305, S306 | The first PCO |
| S307 | On the basis of first security information, establish a secure connection with the DNS server |
| AA | Terminal device |
| BB | Visited session management function network element |
| CC | Home session management function network element |

(57) **Abstract:** Embodiments of the present application provide a communication method and a communication apparatus, applied to a session establishment or modification process of a terminal device. The method comprises: a visited session management function network element acquiring security information of a visited DNS server and an identifier of the DNS server, and sending the security information and the identifier of the DNS server to a home session management function network element; and receiving, from the home session management function network element, a PCO comprising the security information and the identifier of the DNS server,

[见续页]

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))。

then sending the PCO to a terminal device. By means of the solution disclosed in the present application, a visited session management function network element exchanges security information with a home session management function network element, then the home session management function network element sends the security information to a terminal device, so that the terminal device can establish a secure connection with a DNS server according to the security information, thereby improving the network communication security.

**(57)** 摘要: 本申请实施例提供了一种通信方法和通信装置，应用于建立或修改终端设备的会话过程。该方法包括：拜访地的会话管理功能网元获取位于拜访地的DNS服务器的安全信息和DNS服务器的标识，并向归属地的会话管理功能网元发送该安全信息和DNS服务器的标识；以及从归属地的会话管理功能网元接收包括安全信息和DNS服务器的标识的PCO，再将该PCO发送给终端设备。本申请所揭示的方案，通过拜访地的会话管理功能网元与归属地的会话管理功能网元交互安全信息，再由归属地的会话管理功能网元将安全信息发送给终端设备，使得终端设备可以根据安全信息建立与DNS服务器之间的安全连接，从而提高网络通信安全。

# 通信方法和通信装置

本申请要求在 2023 年 01 月 06 日提交中国国家知识产权局、申请号为 202310021264.4 的中国专利申请的优先权，发明名称为“通信方法和通信装置”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

## 技术领域

本申请涉及通信领域，并且更具体地，涉及一种通信方法和通信方法。

## 背景技术

在面向边缘计算的网络系统架构中，支持用户设备（user equipment，UE）接入拜访地公共陆地移动网络（visited public land mobile network，VPLMN）中的边缘托管环境（edge hosting environment，EHE）。

在漫游场景中，UE 可以向拜访地网络发起注册流程，以及协议数据单元（protocol data unit，PDU）会话建立流程，以建立接入拜访地 EHE 的网络连接。在这种情况下，UE 可以通过与拜访地的域名系统（domain name system，DNS）服务器交互获取拜访地 EHE 中的应用服务器地址。如何保护 UE 和 DNS 服务器之间的通信安全，是当前需要考虑的问题。

## 发明内容

本申请提供一种通信方法和通信方法，能够保护拜访地的 DNS 服务器与通信装置之间的通信安全。

第一方面，提供了一种通信方法，该方法可以由拜访地的会话管理功能网元（例如 Visited-session management function，V-SMF，简称 V-SMF）执行，或者，也可以由用于 V-SMF 的芯片或电路执行，本申请对此不作限定。为了便于描述，下面以由 V-SMF 执行为例进行说明。

该方法包括：拜访地的会话管理功能网元获取位于拜访地的域名系统 DNS 服务器的安全信息和 DNS 服务器的标识，安全信息用于终端设备与 DNS 服务器之间建立安全连接；拜访地的会话管理功能网元向归属地的会话管理功能网元发送安全信息和 DNS 服务器的标识；拜访地的会话管理功能网元接收来自归属地的会话管理功能网元的协议配置选项（protocol configuration options，PCO），PCO 包括安全信息和 DNS 服务器的标识；拜访地的会话管理功能网元将 PCO 发送给终端设备。

示例性的，拜访地的 DNS 服务器可以为拜访地的边缘服务器发现功能网元（V-edge application server discovery function，V-EASDF）。可以理解的是，本申请实施例中的 V-EASDF 为 DNS 服务器的增强功能，V-EASDF 能够支持 DNS 服务器所有的功能，并且进行了额外的增强。因此，后续 UE 根据安全信息与 V-EASDF 交互执行服务器发现的流程的具体实现方式，可参考当前 UE 与 DNS 服务器之间交互的实现方式。为了简洁，此处不再过多赘述。

需要说明的是，本申请技术方案主要针对漫游场景，应用于建立或修改终端设备的会话过程中，即终端设备位于拜访地时，建立或修改终端设备的 PDU 会话过程。

根据本申请提供的方案，拜访地的会话管理功能网元获取安全信息，并与归属地的会话管理功能网元交互安全信息，进一步地，从归属地的会话管理功能网元获取包含安全信息的 PCO，并将 PCO 发送给终端设备，使得终端设备可以根据安全信息建立与 DNS 服务器之间的安全连接，可以提高终端设备与 DNS 服务器之间通信的安全性能。

结合第一方面，在第一方面的某些实现方式中，安全信息包括用于认证 DNS 服务器的凭证。

基于该实现方式，通过在安全信息中增加 DNS 服务器的凭证，使得在终端设备与 DNS 服务器建立安全连接过程中对 DNS 服务器执行认证，能够保障网络通信安全。

结合第一方面，在第一方面的某些实现方式中，安全信息还包括 DNS 服务器支持的一种或者多种安全协议类型，和/或建立安全连接所使用的端口号。

基于该实现方式，通过在安全信息中增加 DNS 服务器支持的安全协议类型，和/或建立安全连接所使用的端口号，能够保证终端设备与 DNS 服务器使用正确的安全协议和/或端口号建立安全连接，保障通信

安全连接的建立效率。

结合第一方面，在第一方面的某些实现方式中，在拜访地的会话管理功能网元接收来自归属地的会话管理功能网元的PCO之前，拜访地的会话管理功能网元向归属地的会话管理功能网元发送DNS服务器支持的一种或者多种安全协议类型，和/或建立安全连接所使用的端口号；其中，PCO中还包括DNS服务器支持的一种或者多种安全协议类型中的一个或者多个安全协议类型和/或端口号。

基于该实现方式，通过在PCO中增加DNS服务器支持的安全协议类型，和/或建立安全连接所使用的端口号，能够保证终端设备与DNS服务器使用正确的安全协议和/或端口号建立安全连接，保障通信安全连接的建立效率。

结合第一方面，在第一方面的某些实现方式中，来自归属地的会话管理功能网元的PCO为第一PCO；在拜访地的会话管理功能网元获取位于拜访地的DNS服务器的安全信息之前，拜访地的会话管理功能网元接收来自终端设备的第二PCO，其中，第二PCO包括用于指示终端设备支持基于安全协议对DNS消息进行安全保护的指示信息；拜访地的会话管理功能网元向归属地的会话管理功能网元发送第二PCO；拜访地的会话管理功能网元接收来自归属地的会话管理功能网元的请求消息，请求消息包括用于指示终端设备支持基于安全协议对DNS消息进行安全保护指示信息；其中，拜访地的会话管理功能网元获取位于拜访地的DNS服务器的安全信息，包括：响应于指示信息，拜访地的会话管理功能网元获取安全信息。

基于该实现方式，第二PCO中携带的用于指示终端设备支持基于安全协议对DNS消息进行安全保护的指示信息，通过归属地的会话管理功能网元发送给拜访地的会话管理功能网元，进而使得拜访地的会话管理功能网元根据归属地的会话管理功能网元发送的请求消息，确定并获取DNS服务器的安全信息，增加了拜访地的会话管理功能网元获取DNS服务器的安全信息的考虑因素或依据，使得网络能够按需获取安全信息。

结合第一方面，在第一方面的某些实现方式中，在拜访地的会话管理功能网元获取位于拜访地的DNS服务器的安全信息和DNS服务器的标识之前，拜访地的会话管理功能网元接收来自移动和接入管理功能网元的归属地路由会话疏导（home routed session breakout，HR-SBO）允许指示；其中，拜访地的会话管理功能网元获取位于拜访地的DNS服务器的安全信息和DNS服务器的标识，包括：拜访地的会话管理功能网元根据HR-SBO允许指示，获取安全信息和DNS服务器的标识。

基于该实现方式，拜访地的会话管理功能网元根据移动和接入管理功能网元发送的HR-SBO允许指示，确定并获取DNS服务器的安全信息和DNS服务器的标识，增加了拜访地的会话管理功能网元获取DNS服务器的安全信息和DNS服务器的标识的考虑因素或依据，使得网络能够按需获取安全信息。

结合第一方面，在第一方面的某些实现方式中，所述拜访地的会话管理功能网元获取位于所述拜访地的DNS服务器的安全信息，包括：所述拜访地的会话管理功能网元根据本地配置信息，获取安全信息。

结合第一方面，在第一方面的某些实现方式中，在拜访地的会话管理功能网元获取位于拜访地的DNS服务器的安全信息之前，拜访地的会话管理功能网元接收来自归属地的会话管理功能网元的归属地的网络标识；其中，拜访地的会话管理功能网元获取位于拜访地的DNS服务器的安全信息，包括：拜访地的会话管理功能网元根据终端设备的网络标识，获取安全信息。

基于该实现方式，拜访地的会话管理功能网元根据本地配置信息，或者归属地的会话管理功能网元发送的归属地的网络标识，确定并获取DNS服务器的安全信息，增加了拜访地的会话管理功能网元获取DNS服务器的安全信息的考虑因素或依据，使得网络能够获取准确的安全信息。

结合第一方面，在第一方面的某些实现方式中，拜访地的会话管理功能网元获取策略信息，策略信息用于指示归属地的会话管理功能网元向终端设备发送安全信息的触发条件；拜访地的会话管理功能网元向归属地的会话管理功能网元发送策略信息。

基于该实现方式，拜访地的会话管理功能网元通过向归属地的会话管理功能网元发送策略信息，增加了归属地的会话管理功能网元将安全信息发送给终端设备的触发条件，使得网络能够按需向终端设备提供安全信息。

结合第一方面，在第一方面的某些实现方式中，在拜访地的会话管理功能网元获取位于拜访地的DNS服务器的安全信息之前，拜访地的会话管理功能网元接收来自归属地的会话管理功能网元的与会话对应的用户面安全策略，用户面安全策略指示不开启或者可选开启用户面安全保护；其中，拜访地的会话管理功能网元获取位于拜访地的DNS服务器的安全信息，包括：拜访地的会话管理功能网元根据用户面安全策略，获取安全信息。

基于该实现方式，拜访地的会话管理功能网元根据归属地的会话管理功能网元发送的用户面安全策略，确定并获取 DNS 服务器的安全信息，增加了拜访地的会话管理功能网元获取 DNS 服务器的安全信息考虑因素或依据，使得网络能够按需获取安全信息。

结合第一方面，在第一方面的某些实现方式中，在拜访地的会话管理功能网元获取位于拜访地的 DNS 服务器的安全信息和 DNS 服务器的标识之前，拜访地的会话管理功能网元接收来自归属地的会话管理功能网元的 HR-SBO 授权信息；其中，拜访地的会话管理功能网元获取位于拜访地的 DNS 服务器的安全信息和 DNS 服务器的标识，包括：拜访地的会话管理功能网元根据 HR-SBO 授权信息，获取安全信息和 DNS 服务器的标识。

基于该实现方式，拜访地的会话管理功能网元需要基于来自归属地的会话管理功能网元的 HR-SBO 授权信息，确定并获取安全信息和 DNS 服务器的标识，增加了拜访地的会话管理功能网元获取 DNS 服务器的安全信息和 DNS 服务器的标识的考虑因素或依据，使得安全信息的获取更具有安全性。

结合第一方面，在第一方面的某些实现方式中，拜访地的会话管理功能网元根据 HR-SBO 授权信息，获取安全信息和 DNS 服务器的标识，包括：在确定终端设备满足 HR-SBO 会话建立条件的情况下，拜访地的会话管理功能网元根据 HR-SBO 授权信息，获取安全信息和 DNS 服务器的标识。

基于该实现方式，拜访地的会话管理功能网元需要基于来自归属地的会话管理功能网元的 HR-SBO 授权信息，以及在确定终端设备满足 HR-SBO 会话建立条件的情况下，才确定并获取安全信息和 DNS 服务器的标识，安全性更高。

结合第一方面，在第一方面的某些实现方式中，拜访地的会话管理功能网元接收来自网络功能存储库功能网元的安全信息。

第二方面，提供了一种通信方法，该方法可以由归属地的会话管理功能网元（例如（home management function，HPLMN-SMF），简称 H-SMF）执行，或者，也可以由用于 H-SMF 的芯片或电路执行，本申请对此不作限定。为了便于描述，下面以由 H-SMF 执行为例进行说明。

该方法包括：归属地的会话管理功能网元接收来自拜访地的会话管理功能网元的域名系统 DNS 服务器的安全信息和 DNS 服务器的标识，安全信息用于终端设备与 DNS 服务器之间建立安全连接；归属地的会话管理功能网元生成 PCO，PCO 包括安全信息和 DNS 服务器的标识；归属地的会话管理功能网元通过拜访地的会话管理功能网元向终端设备发送 PCO。

示例性的，DNS 服务器为边缘服务器发现功能网元。

需要说明的是，本申请技术方案主要针对漫游场景，应用于建立或修改终端设备的会话过程中，即终端设备位于拜访地时，建立或修改终端设备的 PDU 会话的过程。

根据本申请提供的方案，归属地的会话管理功能网元通过与拜访地的会话管理功能网元交互安全信息，进一步地，将包含安全信息的 PCO 发送给终端设备，使得终端设备可以根据安全信息建立与 DNS 服务器之间的安全连接，从而保障网络通信安全。

结合第二方面，在第二方面的某些实现方式中，安全信息包括用于认证 DNS 服务器的凭证。

基于该实现方式，基于该实现方式，通过在安全信息中增加 DNS 服务器的凭证，使得在终端设备与 DNS 服务器建立安全连接过程中对 DNS 服务器执行认证，可以提高终端设备与 DNS 服务器之间通信的安全性能。

结合第二方面，在第二方面的某些实现方式中，安全信息还包括 DNS 服务器支持的一种或者多种安全协议类型，和/或建立安全连接所使用的端口号。

基于该实现方式，通过在安全信息中增加 DNS 服务器支持的安全协议类型，和/或建立安全连接所使用的端口号，能够保证终端设备与 DNS 服务器使用正确的安全协议和/或端口号建立安全连接过，保障通信安全连接的建立效率。

结合第二方面，在第二方面的某些实现方式中，在归属地的会话管理功能网元向拜访地的会话管理功能网元发送 PCO 之前，归属地的会话管理功能网元接收来自拜访地的会话管理功能网元的 DNS 服务器支持的一种或者多种安全协议类型，和/或建立安全连接所使用的端口号；其中，PCO 中还包括 DNS 服务器支持的一种或者多种安全协议类型中的一个或者多个安全协议类型和/或端口号。

基于该实现方式，通过在 PCO 中增加 DNS 服务器支持的安全协议类型，和/或建立安全连接所使用的端口号，能够保证终端设备与 DNS 服务器使用正确的安全协议或端口号建立安全连接，保障通信安全连接的建立效率。

结合第二方面，在第二方面的某些实现方式中，归属地的会话管理功能网元向统一数据管理功能网元发送签约数据管理请求消息；归属地的会话管理功能网元接收来自统一数据管理功能网元的签约数据管理响应消息，其中，签约数据管理响应消息包括 HR-SBO 授权信息；其中，归属地的会话管理功能网元生成 PCO，包括：响应于 HR-SBO 授权信息，归属地的会话管理功能网元生成 PCO。

基于该实现方式，归属地需要通过向统一数据管理功能网元查询签约数据，并在确定 HR-SBO 会话授权的情况下生成 PCO，能够保障终端设备与 DNS 服务器之间的安全通信。

结合第二方面，在第二方面的某些实现方式中，在归属地的会话管理功能网元接收来自拜访地的会话管理功能网元的 DNS 服务器的安全信息和 DNS 服务器的标识之前，归属地的会话管理功能网元向拜访地的会话管理功能网元发送 HR-SBO 授权信息，HR-SBO 授权信息用于请求获取安全信息和 DNS 服务器的标识。

基于该实现方式，拜访地的会话管理功能网元需要基于来自归属地的会话管理功能网元的 HR-SBO 授权信息，确定并获取安全信息和 DNS 服务器的标识，增加了拜访地的会话管理功能网元获取 DNS 服务器的安全信息和 DNS 服务器的标识的考虑因素或依据，使得网络能够按需获取安全信息。

结合第二方面，在第二方面的某些实现方式中，归属地的会话管理功能网元生成的 PCO 为第一 PCO；在归属地的会话管理功能网元生成 PCO 之前，归属地的会话管理功能网元接收来自拜访地的会话管理功能网元的第二 PCO，第二 PCO 包括用于指示终端设备支持基于安全协议对 DNS 消息进行安全保护的指示信息；归属地的会话管理功能网元向拜访地的会话管理功能网元发送请求消息，请求消息包括指示信息。

基于该实现方式，第二 PCO 中携带的用于指示终端设备支持基于安全协议对 DNS 消息进行安全保护的指示信息，通过归属地的会话管理功能网元发送给拜访地的会话管理功能网元，进而使得拜访地的会话管理功能网元根据归属地的会话管理功能网元发送的请求消息，确定并获取 DNS 服务器的安全信息，增加了拜访地的会话管理功能网元获取 DNS 服务器的安全信息的考虑因素或依据，使得网络按需获取安全信息。

结合第二方面，在第二方面的某些实现方式中，第二 PCO 还包括终端设备支持的一种或者多种安全协议类型；其中，归属地的会话管理功能网元生成 PCO，包括：归属地的会话管理功能网元根据第二 PCO 中携带的终端设备支持的一种或者多种安全协议类型，以及 DNS 服务器支持的一种或者多种安全协议类型，生成第一 PCO，其中，PCO 包括 DNS 服务器和终端设备都支持的一种或者多种安全协议类型中的一个或者多个安全协议类型。

基于该实现方式，归属地的会话管理功能网元根据 DNS 服务器支持的一种或者多种安全协议类型，以及终端设备支持的一种或者多种安全协议类型，最终确定第一 PCO 中携带的 DNS 服务器和终端设备都支持的一个或多个安全协议类型。通过在第一 PCO 中增加 DNS 服务器和终端设备都支持的安全协议类型，和/或建立安全连接所使用的端口号，能够保证终端设备与 DNS 服务器使用正确的安全协议和/或端口号建立安全连接，保障通信安全连接的建立效率。

结合第二方面，在第二方面的某些实现方式中，在归属地的会话管理功能网元生成 PCO 之前，归属地的会话管理功能网元向拜访地的会话管理功能网元发送用户面安全策略，用户面安全策略用于确定安全信息，其中，用户面安全策略指示不开启或者可选开启用户面安全保护。

基于该实现方式，拜访地的会话管理功能网元根据归属地的会话管理功能网元发送的用户面安全策略，确定并获取 DNS 服务器的安全信息，增加了拜访地的会话管理功能网元获取 DNS 服务器的安全信息的考虑因素或依据，使得网络能够按需获取安全信息。

结合第二方面，在第二方面的某些实现方式中，在归属地的会话管理功能网元生成 PCO 之前，归属地的会话管理功能网元向拜访地的会话管理功能网元发送归属地的网络标识，归属地的网络标识用于确定安全信息。

基于该实现方式，拜访地的会话管理功能网元根据本地配置信息，或者归属地的会话管理功能网元发送的归属地的网络标识，确定并获取 DNS 服务器的安全信息，增加了拜访地的会话管理功能网元获取 DNS 服务器的安全信息的考虑因素或依据，使得网络能够按需获取安全信息。

结合第二方面，在第二方面的某些实现方式中，归属地的会话管理功能网元生成 PCO，包括：归属地的会话管理功能网元接收来自拜访地的会话管理功能网元的策略信息，其中，所述策略信息用于指示所述归属地的会话管理功能网元向所述终端设备发送所述安全信息的触发条件；在满足触发条件的情况

下，归属地的会话管理功能网元生成PCO。

基于该实现方式，拜访地的会话管理功能网元通过向归属地的会话管理功能网元发送策略信息，增加了归属地的会话管理功能网元将安全信息发送给终端设备的触发条件，使得网络能够按需向终端设备提供安全信息。

第三方面，提供了一种通信方法，该方法可以由通信装置执行。可选地，通信装置可以是终端设备，例如手机、汽车、无人机、可穿戴设备等，也可以是终端设备中的芯片。另外，终端设备也可以称为用户设备，因此通信装置也可以是用户设备，或者用户设备中的芯片。本申请对此不作具体限定。

该方法包括：通信装置通过拜访地的会话管理功能网元向归属地的会话管理功能网元发送第二 PCO，第二 PCO 包括用于指示通信装置支持基于安全协议对 DNS 消息进行安全保护的指示信息；通信装置通过拜访地的会话管理功能网元接收来自归属地的会话管理功能网元的第一 PCO，其中，第一 PCO 包括安全信息和位于拜访地的域名系统 DNS 服务器的标识；通信装置基于安全信息建立与 DNS 服务器之间安全连接。

示例性的，DNS服务器为边缘服务器发现功能网元。

需要说明的是，本申请技术方案主要针对漫游场景，应用于建立或修改终端设备的会话过程中，即终端设备位于拜访地时，建立或修改终端设备的PDU会话过程。

根据本申请提供的方案，通信装置从归属地的会话管理功能网元获取包含安全信息的 PCO，并基于该安全信息建立与 DNS 服务器之间的安全连接，可以提高通信装置与 DNS 服务器之间通信的安全性能。

结合第三方面，在第三方面的某些实现方式中，安全信息包括用于认证DNS服务器的凭证。

基于该实现方式，通过在安全信息中增加 DNS 服务器的凭证，使得在通信装置与 DNS 服务器建立安全连接过程中对DNS服务器执行认证，能够保障网络通信安全。

结合第三方面，在第三方面的某些实现方式中，安全信息还包括 DNS 服务器支持的一种或者多种安全协议类型，和/或建立安全连接所使用的端口号。

基于该实现方式，通过在安全信息中增加DNS服务器支持的安全协议类型，和/或建立安全连接所使用的端口号，能够保证通信装置与DNS服务器使用正确的安全协议和/或端口号建立安全连接，保障通信安全连接的建立效率。

结合第三方面，在第三方面的某些实现方式中，第二 PCO 还包括通信装置支持的一种或者多种安全协议类型；其中，第一 PCO还包括DNS服务器支持的一种或者多种安全协议类型中的一个或者多个安全协议类型和/或端口号。

第四方面，提供了一种拜访地的会话管理功能网元，例如 V-SMF。该网元包括：处理单元，用于获取位于拜访地的域名系统 DNS 服务器的安全信息和 DNS 服务器的标识，安全信息用于终端设备与 DNS 服务器之间建立安全连接；收发单元，用于向归属地的会话管理功能网元发送安全信息和 DNS 服务器的标识；收发单元，还用于接收来自归属地的会话管理功能网元的 PCO，PCO 包括安全信息和 DNS服务器的标识；收发单元，还用于将PCO发送给终端设备。

该收发单元可以执行前述第一方面中的接收和发送的处理，处理单元可以执行前述第一方面中除了接收和发送之外的其他处理。

第五方面，提供了一种归属地的会话管理功能网元，例如 H-SMF。该网元包括：收发单元，用于接收来自拜访地的会话管理功能网元的域名系统 DNS 服务器的安全信息和 DNS 服务器的标识，安全信息用于终端设备与 DNS 服务器之间建立安全连接；处理单元，用于生成 PCO，PCO 包括安全信息和 DNS 服务器的标识；收发单元，还用于向拜访地的会话管理功能网元发送 PCO。

该收发单元可以执行前述第二方面中的接收和发送的处理，处理单元可以执行前述第二方面中除了接收和发送之外的其他处理。

第六方面，提供了一种终端设备，例如 UE。该装置包括：收发单元，用于向拜访地的会话管理功能网元发送第二 PCO，第二 PCO 包括用于指示终端设备支持基于安全协议对 DNS 消息进行安全保护的指示信息；收发单元，还用于接收来自拜访地的会话管理功能网元的第一 PCO，其中，第一 PCO 包括安全信息和 DNS服务器的标识；以及处理单元，用于基于安全信息，建立与 DNS服务器之间安全连接。

该收发单元可以执行前述第三方面中的接收和发送的处理，处理单元可以执行前述第三方面中除了接收和发送之外的其他处理。

第七方面，提供了一种通信装置，包括收发器、处理器和存储器，该处理器用于控制收发器收发信

号，该存储器用于存储计算机程序，该处理器用于从存储器中调用并运行该计算机程序，使得该通信装置执行上述第一方面或第二方面或第三方面及其任一种可能实现方式中的方法。

可选地，所述处理器为一个或多个，所述存储器为一个或多个。

可选地，所述存储器可以与所述处理器集成在一起，或者所述存储器与处理器分离设置。

可选地，该通信装置还包括发射机（发射器）和接收机（接收器）。

第八方面，提供了一种通信系统，包括前述的终端设备（例如UE），归属地的会话管理功能网元H-SMF，拜访地的会话管理功能网元V-SMF中的一个或多个。

第九方面，提供了一种计算机可读存储介质，所述计算机可读存储介质存储有计算机程序或代码，所述计算机程序或代码在计算机上运行时，使得所述计算机执行上述第一方面至或第二方面或第三方面及其任一种可能实现方式中的方法。

第十方面，提供了一种芯片，包括至少一个处理器，所述至少一个处理器与存储器耦合，该存储器用于存储计算机程序，该处理器用于从存储器中调用并运行该计算机程序，使得安装有该芯片系统的终端设备执行上述第一方面或第二方面或第三方面及其任一种可能实现方式中的方法。

其中，该芯片可以包括用于发送信息或数据的输入电路或者接口，以及用于接收信息或数据的输出电路或者接口。

第十一方面，提供了一种计算机程序产品，所述计算机程序产品包括：计算机程序代码，当所述计算机程序代码被终端设备运行时，使得所述终端设备执行上述第一方面或第二方面或第三方面及其任一种可能实现方式中的方法。

**附图说明**

图1是本申请实施例适用的网络架构的示意图。

图2是本申请实施例提供的一种HR-SBO PDU会话建立的流程示意图。

图3是本申请实施例提供的通信方法300的流程示例图。

图4是本申请实施例提供的通信方法400的流程示意图。

图5是本申请实施例提供的通信方法500的流程示意图。

图6是本申请实施例提供的通信方法600的流程示意图。

图7是本申请实施例提供的通信方法700的流程示意图。

图8是本申请实施例提供的通信方法800的流程示意图。

图9是本申请实施例提供的一种终端设备1000的结构示意图。

图10是本申请实施例提供的另一种终端设备2000的结构示意图。

图11是本申请实施例提供的一种芯片系统3000的结构示意图。

**具体实施方式**

下面将结合附图，对本申请中的技术方案进行描述。

本申请提供的技术方案可以应用于各种通信系统，例如：新无线（new radio，NR）系统、长期演进（long term evolution，LTE）系统、LTE频分双工（frequency division duplex，FDD）系统、LTE时分双工（time division duplex，TDD）系统等。本申请提供的技术方案还可以应用于设备到设备（device to device，D2D）通信，车到万物（vehicle-to-everything，V2X）通信，机器到机器（machine to machine，M2M）通信，机器类型通信（machine type communication，MTC），以及物联网（internet of things，IoT）通信系统或者其他通信系统。

在通信系统中，由运营者运营的部分可称为PLMN，也可以称为运营商网络等。PLMN是由政府或其所批准的经营者为公众提供陆地移动通信业务目的而建立和经营的网络，主要是移动网络运营商（mobile network operator，MNO）为用户提供移动宽带接入服务的公共网络。本申请实施例中所描述的PLMN，具体可为符合第三代合作伙伴项目（3rd generation partnership project，3GPP）标准要求的网络，简称3GPP网络。3GPP网络通常包括但不限于5G网络、第四代移动通信（4th-generation，4G）网络，以及未来的其他通信系统，例如（6th-generation，6G）网络等。

为了方便描述，本申请实施例中将以5G网络为例进行说明。

图1是本申请实施例适用的网络架构的示意图。如图1的（a）所示，该网络架构具体可以包括三部

分，分别是终端设备部分、数据网络（data network，DN）和运营商网络PLMN部分。下面对各部分的网元的功能进行简单说明。

终端设备部分可以包括终端设备110，该终端设备110也可以称为用户设备（user equipment，UE）。本申请中的终端设备110是一种具有无线收发功能的设备，可以经无线接入网（radio access network，RAN）140中的接入网设备（或者也可以称为接入设备）与一个或多个核心网（core network，CN）设备进行通信。终端设备110也可称为接入终端、终端、用户单元、用户站、移动站、移动台、远方站、远程终端、移动设备、用户终端、用户代理或用户装置等。终端设备110可以部署在陆地上，包括室内或室外、手持或车载；也可以部署在水面上（例如轮船等）；还可以部署在空中（例如飞机、气球和卫星上等）。终端设备110可以是蜂窝电话（cellular phone）、无绳电话、会话启动协议（session initiation protocol，SIP）电话、智能电话（smart phone）、手机（mobile phone）、无线本地环路（wireless local loop，WLL）站、个人数字处理（personal digital assistant，PDA）等。或者，终端设备110还可以是具有无线通信功能的手持设备、计算设备或连接到无线调制解调器的其它设备、车载设备、可穿戴设备、无人机设备或物联网、车联网中的终端、5G网络以及未来网络中的任意形态的终端、中继用户设备或者未来演进的6G网络中的终端等。其中，中继用户设备例如可以是5G家庭网关（residential gateway，RG）。例如终端设备110可以是虚拟现实（virtual reality，VR）终端、增强现实（augmented reality，AR）终端、工业控制（industrial control）中的无线终端、无人驾驶（self driving）中的无线终端、远程医疗（remote medical）中的无线终端、智能电网（smart grid）中的无线终端、运输安全（transportation safety）中的无线终端、智慧城市（smart city）中的无线终端、智慧家庭（smart home）中的无线终端等。这里的终端设备指的是3GPP终端。本申请实施例对终端设备的类型或种类等并不限定。为便于说明，本申请后续以UE代指终端设备为例进行说明。

运营商网络PLMN部分可以包括但不限于（无线）接入网（（radio）access network，（R）AN）120和核心网（core network，CN）部分。

(R)AN 120可以看作是运营商网络的子网络，是运营商网络中业务节点与终端设备110之间的实施系统。终端设备110要接入运营商网络，首先是经过(R)AN 120，进而可通过(R)AN 120与运营商网络的业务节点连接。本申请实施例中的接入网设备（RAN设备），是一种为终端设备110提供无线通信功能的设备，也可以称为网络设备，RAN设备包括但不限于：5G系统中的下一代基站节点（next generation node base station，gNB）、长期演进（long term evolution，LTE）中的演进型节点B（evolved node B，eNB）、无线网络控制器（radio network controller，RNC）、节点B（node B，NB）、基站控制器（base station controller，BSC）、基站收发台（base transceiver station，BTS）、家庭基站（例如，home evolved nodeB，或home node B，HNB）、基带单元（base band unit，BBU）、传输点(transmitting and receiving point，TRP)、发射点(transmitting point，TP)、小基站设备（pico）、移动交换中心，或者未来网络中的网络设备等。采用不同无线接入技术的系统中，具备接入网设备功能的设备的名称可能会有所不同。为方便描述，本申请所有实施例中，上述为终端设备110提供无线通信功能的装置统称为接入网设备或简称为RAN或AN。应理解，本文对接入网设备的具体类型不作限定。

CN部分可以包括但不限于如下网络功能（Network Function，NF)：用户面功能（user plane function，UPF）130、网络开放功能（network exposure function，NEF）131、网络功能存储库功能（network function repository function，NRF）132、策略控制功能（policy control function，PCF）133、统一数据管理功能（unified data management，UDM）134、统一数据存储库功能（unified data repository，UDR）135、网络数据分析功能（network data analytics function，NWDAF）136、认证服务器功能（Authentication Server Function，AUSF）137、接入与移动性管理功能（access and mobility management function，AMF）138、会话管理功能（session management function，SMF）139。

数据网络DN 140，也可以称为分组数据网络（packet data network，PDN），通常是位于运营商网络之外的网络，例如第三方网络。当然，在一些实现方式中，DN也可以由运营商进行部署，即DN属于PLMN中的一部分。本申请对DN是否属于PLMN不作限制。运营商网络PLMN可以接入多个数据网络DN 140，数据网络DN 140上可部署多种业务，可为终端设备110提供数据和/或语音等服务。例如，数据网络DN 140可以是某智能工厂的私有网络，智能工厂安装在车间的传感器可以是终端设备110，数据网络DN 140中部署了传感器的控制服务器，控制服务器可为传感器提供服务。传感器可与控制服务器通信，获取控制服务器的指令，根据指令将采集的传感器数据传送给控制服务器等。又例如，数据网络DN

140 可以是某公司的内部办公网络，该公司员工的手机或者电脑可为终端设备 110，员工的手机或者电脑可以访问公司内部办公网络上的信息、数据资源等。终端设备 110 可通过运营商网络提供的接口（例如 N1 等）与运营商网络建立连接，使用运营商网络提供的数据和/或语音等服务。终端设备 110 还可通过运营商网络访问数据网络 DN 140，使用数据网络 DN 140 上部署的运营商业务，和/或第三方提供的业务。

下面对 CN 包含的 NF 功能进行进一步简要说明。

1、UPF 130 是由运营商提供的网关，是运营商网络与数据网络 DN 140 通信的网关。UPF 网络功能 130 包括数据包路由和传输、数据包检测、业务用量上报、服务质量（quality of service，QoS）处理、合法监听、上行数据包检测、下行数据包存储等用户面相关的功能。

2、NEF 131 是由运营商提供的控制面功能，主要使能第三方使用网络提供的服务，支持网络开放其能力、事件及数据分析、从外部应用给 PLMN 安全配备信息、PLMN 内外交互信息的转换等。

3、NRF 132 是由运营商提供的控制面功能，可用于维护网络中网络功能、服务的实时信息。例如支持网络服务发现、维护 NF 实例的 NF 配置数据（NF profile）支持的服务、支持通信代理（service communication proxy，SCP）的服务发现、维护 SCP 实例的 SCP 配置数据（SCP profile）、发送有关新注册、去注册、更新的 NF 和 SCP 的通知、维护 NF 和 SCP 运行的健康状态等。

4、PCF 133 是由运营商提供的控制面功能，它支持统一的策略框架来治理网络行为、向其他控制功能提供策略规则、策略决策相关的签约信息等。

5、UDM 134 是由运营商提供的控制面功能，负责存储运营商网络中签约用户的用户永久标识符（subscriber permanent identifier，SUPI）、签约用户的公开使用的签约标识（generic public subscription identifier，GPSI），信任状（credential）等信息。其中 SUPI 在传输过程中会先进行加密，加密后的 SUPI 被称为隐藏的用户签约标识符(subscription concealed identifier，SUCI)。UDM 网络功能 134 所存储的这些信息可用于终端设备 110 接入运营商网络的认证和授权。其中，上述运营商网络的签约用户具体可为使用运营商网络提供的业务的用户，例如使用中国电信的手机芯卡（subscriber identity module，SIM）卡的用户，或者使用中国移动的手机芯卡的用户等。上述签约用户的信任状可以是手机芯卡中存储的长期密钥或者跟手机芯卡加密相关的信息等存储的小文件，用于认证和/或授权。需要说明的是，永久标识符、信任状、安全上下文、认证数据（cookie）、以及令牌等同验证/认证、授权相关的信息，在本申请实施例中，为了描述方便起见不做区分、限制。

6、UDR 135 是由运营商提供的控制面功能，为 UDM 提供存储和获取签约数据的功能、为 PCF 提供存储和获取策略数据、存储和获取用户的 NF 群组 ID（group ID）信息等。

7、NWDAF 136 是由运营商提供的控制面功能，其主要功能是从 NF、外部应用功能（application function，AF）以及运维管理（operations，administration and maintenance，OAM）系统等处收集数据，对 NF 和 AF 提供 NWDAF 业务注册、数据开放和分析数据等。

8、AUSF 137 是由运营商提供的控制面功能，通常用于一级认证，即终端设备 110（签约用户）与运营商网络之间的认证。AUSF 网络功能 137 接收到签约用户发起的认证请求之后，可通过 UDM 网络功能 134 中存储的认证信息和/或授权信息对签约用户进行认证和/或授权，或者通过 UDM 网络功能 134 生成签约用户的认证和/或授权信息。AUSF 网络功能 137 可向签约用户反馈认证信息和/或授权信息。

9、AMF 138 是由运营商网络提供的控制面网络功能，负责终端设备 110 接入运营商网络的接入控制和移动性管理，例如包括移动状态管理，分配用户临时身份标识，认证和授权用户等功能。

10、SMF 139 是由运营商网络提供的控制面网络功能，负责管理终端设备 110 的 PDU 会话。PDU 会话是一个用于传输 PDU 的通道，终端设备需要通过 PDU 会话与数据网络 DN 140 互相传送 PDU。PDU 会话由 SMF 网络功能 139 负责建立、维护和删除等。SMF 网络功能 139 包括会话管理（例如会话建立、修改和释放，包含用户面功能 UPF 130 和(R)AN 120 之间的隧道维护）、UPF 网络功能 130 的选择和控制、业务和会话连续性（service and session continuity，SSC）模式选择、漫游等会话相关的功能。

在面向边缘计算的 5G 系统架构中，正在定义增强 5GS 支持 UE 接入 VPLMN 中的 EHE，例如 UE 通过建立的本地疏导 PDU（local breakout PDU，LBO PDU）会话接入 VPLMN 中的 EHE（可以简称 V-EHE）；或者，UE 通过建立的归属地路由 PDU（home routed PDU，HR PDU）会话接入 V-EHE。其中，HR PDU 会话是指归属地路由 PDU 会话，该类型的 PDU 会话由归属网络（home PLMN，HPLMN）控制的 SMF、VPLMN 控制的 SMF、HPLMN 控制的至少一个 UPF 和 VPLMN 控制的至少一个 UPF 支持。在这种情况下，HPLMN 中的 SMF 选择 HPLMN 中的 UPF，VPLMN 中的 SMF 选择 VPLMN 中的 UPF。

示例性的，针对UE通过建立的HR PDU会话接入V-EHE，定义了如图1的（b）所示的漫游架构，该网络架构具体可以包括VPLMN和HPLMN两部分，其中涉及的网元的功能可以参考上述图1的（a）相关描述，为了简洁，此处不再过多赘述。在该网络架构中，UE可以建立HR PDU会话，并在VPLMN中插入上行分类器/分支点（uplink classifier/branching point，UL CL/BP），从而支持UE接入VPLMN中的EHE（例如图1的（b）中的边缘应用服务器（edge application server，EAS），这种类型的HR PDU会话可以称为归属地路由会话疏导PDU会话（HR session breakout PDU，HR-SBO PDU）会话。可选地，HR-SBO PDU会话在VPLMN中可以仅包含UL CL/BP的UPF和L-PSA的UPF。可选地，UL CL/BP的UPF和L-PSA的UPF还可以共部署。即一个UPF既作为UL CL的UPF，又作为L-PSA的UPF。

下面对图1的（b）中的部分网元的功能进行简单说明。

1、边缘应用服务器发现功能EASDF：一种部署在运营商网络中的网元（DNS服务器），用于根据SMF的指示处理DNS消息，具体包含以下一项或多项：接收DNS消息处理规则，与UE交互DNS消息，将DNS消息发送给中心DNS或者本地DNS，缓存或丢弃来自UE或DNS服务器的DNS消息等。若使用DNS安全，则EASDF还可以用于终结DNS安全。一个PLMN中可以部署一个或多个EASDF实例。EASDF与PSA UPF在N6上有直接的用户面连接，用于传输与UE交换的DNS信令。

2、EHE可以部署在DN中。EHE可以由运营商控制或者第三方控制，EHE中可以部署一个或多个EAS。

可以理解的是，上述网元或者功能既可以是硬件设备中的物理实体，也可以是在专用硬件上运行的软件实例，或者是共享平台（例如，云平台）上实例化的虚拟化功能。简单来说，一个NF可以由硬件来实现，也可以由软件来实现。

图1中Nnef、Nnrf、Npcf、Nudm、Nudr、Nnwdaf、Nausf、Namf、Nsmf、Neasdf、N1、N2、N3、N4、N6以及N9为接口序列号。示例性的，上述接口序列号的含义可参见3GPP标准协议中定义的含义，本申请对于上述接口序列号的含义不做限制。需要说明的是，图1中的各个网络功能之间的接口名称仅仅是一个示例，在具体实现中，该系统架构的接口名称还可能为其他名称，本申请对此不作限定。此外，上述各个网元之间的所传输的消息（或信令）的名称也仅仅是一个示例，对消息本身的功能不构成任何限定。

应理解，图1中所示的AMF、SMF、UPF、NEF、AUSF、NRF、PCF、UDM可以理解为核心网中用于实现不同功能的网元，例如可以按需组合成网络切片。这些核心网网元可以各自独立的设备，也可以集成于同一设备中实现不同的功能，本申请对于上述网元的具体形态不作限定。

还应理解，上述命名仅为便于区分不同的功能而定义，不应对本申请构成任何限定。本申请并不排除在5G网络以及未来其它的网络中采用其他命名的可能。例如，在6G网络中，上述各个网元中的部分或全部可以沿用5G中的术语，也可能采用其他名称等。

下面，对HR-SBO PDU会话建立过程进行简单说明，具体描述可以参见3GPP TS23.548。

在一种可能的实现方式中，在HR-SBO PDU会话建立过程中，由V-SMF确定和选择V-EASDF，并与V-EASDF建立DNS上下文。具体包括如下实现过程。

在3GPP TS23.502定义的注册流程中，UE请求注册到网络中，并且AMF通过Nudm_UDM_Get服务接收来自UDM的每个数据网络名称（data network name，DNN）或者单网络切片选择支撑信息（single network slice selection assistance information，S-NSSAI）对应的HR-SBO允许指示。

在3GPP TS23.502定义的PDU会话建立流程中，如果AMF在UE注册请求过程中接收到针对请求的DNN/S-NSSAI的HR-SBO允许指示，则AMF可以为UE选择支持HR-SBO的V-SMF。进一步地，V-SMF向H-SMF发送建立VPLMN中支持HR-SBO的PDU会话的请求和V-EASDF地址。

然后，H-SMF根据会话管理签约数据对V-SMF的请求进行授权，并向V-SMF提供可选的VPLMN特定的卸载策略（如果HPLMN中基于HPLMN和VPLMN之间的SLA存在）和HPLMN的DNS服务器地址。其中，H-SMF将DNS服务器地址字段设置为V-EASDF地址，携带在PCO中发送给V-SMF。

最后，V-SMF根据接收来自H-SMF的VPLMN特定卸载策略和HPLMN的DNS服务器地址，向V-EASDF配置DNS处理规则。

图2是本申请实施例提供的一种HR-SBO PDU会话建立流程200的示意图。如图2所示，该方法包括如下多个步骤，未详尽说明的部分可参考现有协议。

S201，UE向AMF发送注册请求；对应的，AMF接收来自UE的注册请求。

示例性的，UE 向 AMF 发送 Registration Request 消息，用于请求注册到网络中。

S202，AMF 向 UDM 请求获取签约数据管理（subscriber data management，SDM）信息（Get SDM information）；对应的，UDM 接收来自 AMF 的用于获取 SDM 信息的请求。

S203，UDM 向 AMF 发送 SDM 信息（SDM information）；对应的，AMF 接收来自 UDM 的 SDM 信息。

其中，SDM 信息中携带基于数据网络名称（data network name，DNN）/单网络切片选择支撑信息（single network slice selection assistance information，S-NSSAI）的 HR-SBO 允许指示（HR-SBO allowed indication），即允许 UE 使用 DNN/S-NSSAI 对应的归属地路由的 PDU 会话接入 VPLMN 中的数据网络或本地数据网络。

示例性的，AMF 可以通过 Nudm_UDM_Get 服务接收来自 UDM 的基于 per DNN/S-NSSAI 的 HR-SBO 允许指示。

S204，AMF 向 UE 发送注册响应；对应的，UE 接收来自 AMF 的注册响应。

响应于步骤 S201 的注册请求，AMF 向 UE 发送 Registration Response 消息。

即，上述步骤 S201 至 S204 是 UE 注册到网络中的过程，具体实现方式可参考 3GPP TS23.502 中的相关描述，为了简洁，此处不再过多赘述。

S205，UE 向 AMF 发送 PDU 会话建立请求；对应的，AMF 接收来自 UE 的 PDU 会话建立请求。

示例性的，UE 向 AMF 发送 PDU session establishment request 消息和 DNN/S-NSSAI。进一步地，AMF 根据该 PDU 会话的 DNN/S-NSSAI，与上述注册过程中获取的基于 DNN/S-NSSAI 的 HR-SBO 允许指示，确定为 PDU 会话选择支持 HR-SBO 的 V-SMF。即，在确定 UE 请求的 PDU 会话允许 HR-SBO 时，AMF 选择支持该 HR-SBO 的 V-SMF。

S206，AMF 向 V-SMF 发送创建会话管理上下文请求；对应的，V-SMF 接收来自 AMF 的创建会话管理上下文请求。

S207，V-SMF 向 AMF 发送创建会话管理上下文响应；对应的，AMF 接收来自 V-SMF 的创建会话管理上下文响应。

示例性的，AMF 向 V-SMF 发送 CreatSMContext Request 消息，该消息可以携带 N1 SM 容器，N1 SM 容器包含 PDU 会话建立。可选地，该消息还可以携带 HR-SBO 允许指示；对应的，AMF 接收来自 V-SMF 的 CreatSMContext Response 消息。

S208，V-SMF 向 H-SMF 发送创建 HR-SBO 会话请求；对应的，H-SMF 接收来自 V-SMF 的创建 HR-SBO 会话请求。

其中，创建 HR-SBO 会话请求中携带 HR-SBO 请求、V-EASDF 的地址或 VPLMN 的 DNS 服务器的地址（可以简称 V-DNS server address），例如 IP 地址（如可以是 IPv4 地址或 IPv6 前缀或 IPv6 地址）。

示例性的，在 V-SMF 确定创建 HR VSBO 会话的情况下，V-SMF 向 H-SMF 发送包含 VSBO 请求、V-EASDF 地址或 V-DNS 服务器地址的 PDU session Creat Request 消息。

S209，H-SMF 向 UDM 请求获取 SDM 信息；对应的，UDM 接收来自 H-SMF 的获取 SDM 信息的请求。

S210，UDM 向 H-SMF 发送 SDM 信息；对应的，H-SMF 接收来自 UDM 的 SDM 信息。

其中，SDM 信息中包含允许的 HR-SBO（HR-SBO allowed），例如可以是 HR-SBO 授权指示，和/或 HR-SBO 授权信息。

可选地，允许的 HR-SBO 指示也可以（预）配置在 H-SMF 中，则上述步骤 S209 和 S210 从 UDM 获取允许的 HR-SBO 的流程可以不执行。

S211，H-SMF 向 V-SMF 发送创建 HR-SBO 会话响应；对应的，V-SMF 接收来自 H-SMF 的创建 HR-SBO 会话响应。

其中，创建 HR-SBO 会话响应包括 HR-SBO 的授权指示、协议配置选项（protocol configuration option，PCO）和归属 DNS 服务器的地址。

示例性的，在 H-SMF 确定允许建立 HR-SBO PDU 会话的情况下，H-SMF 将 PCO 中的 DNS 服务器地址设置为 V-EASDF 的地址，并向 V-SMF 发送包含 HR-SBO 允许指示，PCO，归属 DNS 服务器地址的 PDU session Creat Response 消息。

S212，V-SMF 触发本地 UPF 插入 ULCL/BP。

S213，V-SMF 向 V-EASDF 发送 DNS 上下文创建请求；对应的，V-EASDF 接收来自 V-SMF 的 DNS 上下文创建请求。

示例性的，DNS 上下文创建请求可以是 Neasdf_DNSContextCreat Request 消息，例如请求中包括 DNS 消息处理规则（DNS Message Handling Rule），UE IP 地址，DNN。

S214，V-SMF 向 AMF 发送 N1N2 消息传输；对应的，AMF 接收来自 V-SMF 的 N1N2 消息传输。

其中，N1N2 消息传输可以是 N1N2_MessageTransfer，该消息包含 PDU 会话建立接收或拒绝的信息（PDU session Establishment Accept/Reject）。

S215，AMF 向 UE 发送 PDU 会话建立接收或拒绝；对应的，UE 接收来自 AMF 的 PDU 会话建立接收或拒绝。

即，上述步骤 S205 至 S215 是 UE 请求 PDU 会话建立的过程，具体实现方式可参考 3GPP TS23.502 中的相关描述，为了简洁，此处不再过多赘述。

进一步，基于上述 HR-SBO PDU 会话建立流程，后续 UE 可以与 V-EASDF 交互 DNS 消息，以发现应用服务器的地址。为了保障网络通信安全，DNS 消息的安全保护是需要考虑的问题。

示例性的，根据 3GPP TS33.501 定义了一种保护 DNS 消息的安全措施，可以用于用户面完整性保护无法使用的情况下。其中，具体的安全方法包括 UE 和 DNS 服务器支持基于(D)TLS 的 DNS。部署在 3GPP 网络中的 NDS 服务器能够强制使用基于(D)TLS 的 DNS 保护机制。UE 可以预配置 DNS 服务器的安全信息，或者接收来自核心网的 DNS 服务器的安全信息，以便于在使用基于(D)TLS 的 DNS 的情况下，需要协商支持完整性保护的 TLS 密码套件。基于 3GPP TS24.501 的相关描述，可以实现上述通过核心网提供 DNS 服务器的安全信息。例如，UE 可以在 PDU 会话建立请求消息（例如，上述方法 200 的步骤 S205）中携带扩展协议配置选项（extended protocol configuration options，ePCO）信息元（information element，IE），以及 DNS 服务器的安全信息指示符。可选地，PDU 会话建立请求消息还可以携带 DNS 服务器的安全协议支持，用于指示 UE 希望支持的安全协议类型。对应的，网络可以在向 UE 发送的 PDU 会话建立接受消息中携带 ePCO IE，包括长度为两个八位字节的 DNS 服务器的安全信息。可选地，PDU 会话建立接受消息还可以携带 DNS 服务器的安全协议支持，表示网络希望 UE 强制使用 DNS over (D)TLS。UE 在接收到 DNS 服务器的安全信息后，应将其传递给上层，以及 UE 可以使用 DNS 服务器的安全信息，通过(D)TLS 发送 DNS 消息。

应理解，上述保护 DNS 消息的方案主要适应于非漫游 PDU 会话或者 LBO 会话场景中，也就是说，由 SMF 根据 ePCO 中携带的 UE 支持的 DNS over (D)TLS 能力，可选地，UE 支持的安全协议类型等信息，选择 EASDF 作为 DNS 服务器，并向 UE 提供 EASDF 的安全信息。然而，针对漫游场景下，当 PDU 会话有两个服务的 SMF 时，例如 HR PDU 会话，由 V-SMF 和 H-SMF 来管理该 HR PDU 会话，如何确定向 UE 提供 DNS 服务器的安全信息尚未定义。

具体来说，针对增强的边缘计算架构中的 HR-SBO 的 PDU 会话场景，可以由 V-SMF 确定 V-EASDF 作为 DNS 服务器，由于 ePCO 在 PDU 会话建立过程中由 V-SMF 透传给 H-SMF，V-SMF 并不解析 ePCO 的内容，因此 V-SMF 无法感知 UE 是否支持 DNS over (D)TLS，以及 UE 支持哪种安全协议类型，从而无法确定是否使用 DNS over (D)TLS。相比而言，H-SMF 能够获取 UE 是否支持 DNS over (D)TLS，以及 UE 支持哪种安全协议类型，但是 H-SMF 并不感知 V-EASDF 的信息。当建立的 HR PDU 会话的用户面安全（如完整性保护）未开启时，网络无法为 UE 与 V-EASDF 之间交互的 DNS 消息提供安全保护。

换言之，在漫游架构中，针对支持 UE 通过 HR PDU 会话接入 V-EHE 的场景，若 V-SMF 确定使用 V-EASDF 处理 DNS 消息时，如何保证 UE 与 V-EASDF 之间的 DNS 消息安全是亟待解决的技术问题。

有鉴于此，本申请提供了一种通信方法和装置，针对支持终端设备接入拜访网络中的边缘环境的会话建立或修改的过程，通过拜访地的会话管理功能网元与归属地的会话管理功能网元交互安全信息，再由归属地的会话管理功能网元将安全信息发送给终端设备，使得终端设备可以根据安全信息建立与 DNS 服务器之间的安全连接，从而保障网络通信安全。

为了便于理解本申请实施例，做出以下几点说明：

第一、在本申请中，如果没有特殊说明以及逻辑冲突，不同的实施例之间的术语和/或描述具有一致性、且可以相互引用，不同的实施例中的技术特征根据其内在的逻辑关系可以组合形成新的实施例。

第二、在本申请中，“至少一个”是指一个或者多个，“多个”是指两个或两个以上。“和/或”，描述关联对象的关联关系，表示可以存在三种关系，例如，A 和/或 B，可以表示：单独存在 A，同时存在 A 和

B，单独存在 B 的情况，其中 A，B 可以是单数或者复数。在本申请的文字描述中，字符“/”一般表示前后关联对象是一种“或”的关系。“以下至少一项(个)”或其类似表达，是指的这些项中的任意组合，包括单项（个）或复数项（个）的任意组合。例如，a、b 和 c 中的至少一项（个），可以表示：a，或，b，或，c，或，a 和 b，或，a 和 c，或，b 和 c，或，a、b 和 c。其中 a、b 和 c 分别可以是单个，也可以是多个。

第三、在本申请中，“第一”、“第二”以及各种数字编号（例如，#1、#2 等）指示为了描述方便进行的区分，并不用来限制本申请实施例的范围。例如，区分不同的消息等，而不是用于描述特定的顺序或先后次序。应理解，这样描述的对象在适当情况下可以互换，以便能够描述本申请的实施例以外的方案。

第四、在本申请中，“当……时”、“在……的情况下”以及“如果”等描述均指在某种客观情况下设备会做出相应的处理，并非是限定时间，且也不要求设备在实现时一定要有判断的动作，也不意味着存在其它限定。

第五、在本申请中，术语“包括”和“具有”以及他们的任何变形，意图在于覆盖不排他的包含，例如，包含了一系列步骤或单元的过程、方法、系统、产品或设备不必限于清楚地列出的那些步骤或单元，而是可包括没有清楚地列出的或对于这些过程、方法、产品或设备固有的其它步骤或单元。

第六、在本申请中，“用于指示”可以包括用于直接指示和用于间接指示。当描述某一指示信息用于指示 A 时，可以包括该指示信息直接指示 A 或间接指示 A，而并不代表该指示信息中一定携带有 A。

本申请实施例涉及的指示方式应理解为涵盖可以使得待指示方获知待指示信息的各种方法。待指示信息可以作为整体一起发送，也可以分成多个子信息分开发送，而且这些子信息的发送周期和/或发送时机可以相同，也可以不同，本申请对具体的发送方法不作限定。

本申请实施例中的“指示信息”可以是显式指示，即通过信令直接指示，或者根据信令指示的参数，结合其他规则或结合其他参数或通过推导获得。也可以是隐式指示，即根据规则或关系，或根据其他参数，或推导获得。本申请对此不作具体限定。

第七、在本申请中，“协议”可以是指通信领域的标准协议，例如可以包括 5G 协议、NR 协议以及应用于未来的通信系统中的相关协议，本申请对此不做限定。“预定义”可以包括预先定义。例如，协议定义。“预配置”可以通过在设备中预先保存相应的代码、表格或其他可用于指示相关信息的方式来实现，本申请对于其具体的实现方式不做限定。

第八、在本申请中，“存储”可以是指保存在一个或者多个存储器中。所述一个或者多个存储器可以是单独的设置，也可以是集成在编码器或者译码器、处理器、或终端设备中。所述一个或者多个存储器，也可以是一部分单独设置，一部分集成在译码器、处理器、或终端设备中。存储器的类型可以是任意形式的存储介质，本申请并不对此限定。

第九、在本申请中，“通信”还可以描述为“数据传输”、“信息传输”、“数据处理”等。“传输”包括“发送”和“接收”。

下文将结合附图详细说明本申请实施例提供的通信方法，如可以应用于上述图 1 所示的通信系统中。为了方便描述，本申请实施例中将 HPLMN 中的 SMF 记为 H-SMF，将 vPLMN 中的 SMF 记为 V-SMF，以下相关部分不再赘述。通过拜访地的 V-SMF 获取 DNS 服务器的安全信息，并与归属地的 H-SMF 进行信息交互，进一步的 H-SMF 将 DNS 服务器的安全信息发送给终端设备，以便后续终端设备与 DNS 服务器之间进行安全通信。具体实现方式可参考以下方法 300 至方法 800 部分的描述。

图 3 是本申请实施例提供的通信方法 300 的流程示例图。如图 3 所示，该方法应用于漫游场景下建立或修改终端设备的会话过程，包括如下多个步骤，未详尽说明的部分可参考现有协议。

S301，终端设备向拜访地的会话管理功能网元发送第二 PCO；

对应的，拜访地的会话管理功能网元接收来自终端设备的第二 PCO。

其中，第二 PCO 包括用于指示终端设备支持基于安全协议对 DNS 消息进行安全保护的指示信息。

在本申请实施例中，在终端设备支持基于安全协议对 DNS 消息进行安全保护时，终端设备在第二 PCO 中携带用于指示终端设备支持基于安全协议对 DNS 消息进行安全保护的指示信息。

可选地，第二 PCO 还包括终端设备支持的一种或者多种安全协议类型，或者说，用于指示终端设备支持的安全协议类型。例如，数据报传输层安全（datagram transport layer security，DTLS）和/或传输层安全协议（transport layer security，TLS），还可以是其他安全协议类型，本申请对此不作限定。因此，在本申请实施例中，安全协议类型也可以理解为支持的安全能力信息。

示例性的，终端设备（例如 UE）通过 PDU session Establishment Request 消息向移动管理功能网元

（例如 AMF）发送第二 PCO，AMF 通过 Nsmf_PDUSession_CreatSMContext Request 消息向拜访地的会话管理功能网元（例如 V-SMF）发送第二 PCO。

为了便于说明，本申请实施例将来自归属地的会话管理功能网元的 PCO 为第一 PCO，将来自终端设备的 PCO 为第二 PCO，以下相关部分不再赘述。可选地，第一 PCO 或第二 PCO 可以是扩展的协议配置选项（extended protocol configuration option，ePCO），本申请对此不作限定。

应理解，该方法可以由终端设备执行（例如图 1 所示的 UE），也可以是终端设备中的芯片或电路执行；拜访地的会话管理功能网元可以是图 1 所示的 5G 场景下的 V-SMF，当然不限于 5G 场景中，也可以是后续演进系统中具有类似的功能的网元，为便于表达，本申请后续实施例以 V-SMF 为例。

S302，拜访地的会话管理功能网元获取拜访地的 DNS 服务器的安全信息和 DNS 服务器的标识。

其中，安全信息包括用于认证 DNS 服务器的凭证，例如 DNS 服务器的根密钥；DNS 服务器的标识可以是用于指示 DNS 地址的标识，例如 IP 地址，IP 地址可以是 IPv4 地址，或者 IPv6 前缀，或者 IPv6 地址。

在一种示例中，安全信息还包括 DNS 服务器支持的一种或者多种安全协议类型，和/或建立安全连接所使用的端口号。

在另一种示例中，拜访地的会话管理功能网元还获取 DNS 服务器支持的一种或多种安全协议类型，和/或建立安全连接所使用的端口号。即拜访地的会话管理功能网元获取拜访地的 DNS 服务器的安全信息，DNS 服务器支持的一种或者多种安全协议类型，和/或建立安全连接所使用的端口号，以及 DNS 服务器的标识。

基于上述两种示例，DNS 服务器支持的一种或者多种安全协议类型，和/或建立安全连接所使用的端口号与安全信息可以是包含关系，也可以并列关系，本申请对此不作具体限定。

示例性的，本申请实施例中的 DNS 服务器可以是 V-EASDF。应理解，V-EASDF 可以理解是 DNS 服务器的增强，V-EASDF 能够支持 DNS 服务器所有的功能，并且进行了额外的增强。因此，后续 UE 根据安全信息与 V-EASDF 交互执行服务器发现的流程的具体实现方式，可参考当前 UE 与 DNS 服务器之间交互的实现方式。为了简洁，此处不再过多赘述。

可以理解的是，安全信息用于终端设备与 DNS 服务器之间建立安全连接。也就是说，在终端设备确定发起 DNS 发现流程时，终端设备可以根据接收到的安全信息与 DNS 服务器之间建立(D)TLS 连接，并使用(D)TLS 连接发送 DNS 消息。应理解，该 DNS 消息是被保护的，可以保证 UE 与 DNS 服务器之间的安全通信。

可选地，该安全信息可以是拜访地的会话管理功能网元从网络功能存储库功能网元获取的。

示例性的，拜访地的会话管理功能网元向网络功能存储库功能网元发送 DNS 服务器发现消息，拜访地的会话管理功能网元接收来自网络功能存储库功能网元的响应消息，响应消息中包含安全信息。

可选地，该安全信息还可以是拜访地的会话管理功能网元从本地配置获取。

下面针对安全信息和 DNS 服务器的标识的获取实现方式进行具体说明。

在一种可能的实现方式中，在拜访地的会话管理功能网元获取位于拜访地的 DNS 服务器的安全信息之前，拜访地的会话管理功能网元接收来自终端设备的第二 PCO，其中，第二 PCO 包括用于指示终端设备支持基于安全协议对 DNS 消息进行安全保护的指示信息；拜访地的会话管理功能网元向归属地的会话管理功能网元发送第二 PCO；拜访地的会话管理功能网元接收来自归属地的会话管理功能网元的请求消息，请求消息包括用于指示终端设备支持基于安全协议对 DNS 消息进行安全保护指示信息。进一步地，响应于指示信息，拜访地的会话管理功能网元获取安全信息。

需要说明的是，归属地的会话管理功能网元从终端设备接收到的指示信息，以及归属地的会话管理功能网元向拜访地的会话管理功能网元发送的指示信息可以不同。例如，归属地的会话管理功能网元在接收到来自终端设备的指示信息#1 后，通过解析并生成指示信息#2，然后向拜访地的会话管理功能网元发送的指示信息#2。其中，指示信息#1 和指示信息#2 都是用于指示终端设备支持基于安全协议（例如 DTLS 和/或 TLS）对 DNS 消息进行安全保护。

在本申请实施例中，第二 PCO 包括的用于指示终端设备支持基于安全协议对 DNS 消息进行安全保护的指示信息，即表示终端设备能够支持的安全协议的能力信息，也可以理解为终端设备期望的 DNS 服务器安全信息指示（DNS server security information indicator）。

可选地，来自归属地的会话管理功能网元的请求消息例如 Nsmf_Info Request，本身可以是用于请求

从拜访地的会话管理功能网元获取该安全信息的消息，则此时该请求消息中可以不携带指示信息。

示例性的，拜访地的会话管理功能网元根据接收到的请求消息，或者请求消息中携带的指示信息，确定使用 DNS over (D)TLS，进而可以确定获取安全信息。例如，拜访地的会话管理功能网元从本地或 NRF 获取 DNS 服务器的实例标识，安全信息和 DNS 服务器地址；再例如，拜访地的会话管理功能网元从本地或 NRF 先获取 DNS 服务器的实例标识，再根据 DNS 服务器的实例标识从地址解析器获取 DNS 服务器的地址，以及根据 DNS 服务器的实例标识从 DNS 服务器或其他存储网元或本地获取安全信息；又例如，拜访地的会话管理功能网元先从本地或 NRF 获取 DNS 服务器的实例标识和安全信息，再根据 DNS 服务器的实例标识从地址解析器获取 DNS 服务器的地址。

可选地，请求消息还可以包括以下一项或者多项：PDU 会话的用户面安全策略，HPLMN ID，DNS 服务器安全协议支持（DNS server security protocol support）。

在一种示例中，请求消息中包含 PDU 会话的用户面安全策略，则拜访地的会话管理功能网元可以根据 PDU 会话的用户面安全策略，确定是否提供 DNS 服务器的安全信息。例如，在 PDU 会话的用户面安全策略指示不需要用户面的完整性保护的情况下，拜访地的会话管理功能网元可以确定使用 DNS over (D)TLS，则拜访地的会话管理功能网元可以提供安全信息；或者，若 PDU 会话的用户面安全策略指示需要用户面的完整性保护时，则拜访地的会话管理功能网元可以不提供安全信息。

在另一种示例中，请求消息中包含 HPLMN ID，则拜访地的会话管理功能网元可以根据 HPLMN ID 确定提供 DNS 服务器的安全信息，该安全信息用于 HPLMN ID 对应的 PLMN 中的签约用户与 DNS 服务器进行安全的消息交互。

在又一种示例中，请求消息中包含 DNS 服务器安全协议支持，则拜访地的会话管理功能网元可以根据 DNS 服务器安全协议支持，确定使用 DNS over (D)TLS，并提供安全信息。

需要说明的是，上述提供的示例可以独立实现，也可以组合实现。示例性的，拜访地的会话管理功能网元可以根据本地策略，以及 PDU 会话的用户面安全策略，是否提供 DNS 服务器的安全信息。例如，本地策略指示在终端设备支持 DNS over (D)TLS，且终端设备属于该 HPLMN 的情况下，拜访地的会话管理功能网元可以提供用于 PLMN 中的终端设备与 DNS 服务器进行安全交互的安全信息等。

在另一种可能的实现方式中，在拜访地的会话管理功能网元获取位于拜访地的 DNS 服务器的安全信息和 DNS 服务器的标识之前，拜访地的会话管理功能网元接收来自移动和接入管理功能网元的归属地路由会话疏导 HR-SBO 允许指示。进一步地，拜访地的会话管理功能网元根据 HR-SBO 允许指示，获取安全信息和 DNS 服务器的标识。

示例性的，拜访地的会话管理功能网元从本地或 NRF 获取 DNS 服务器的实例标识，安全信息和 DNS 服务器地址；或者，拜访地的会话管理功能网元从本地或 NRF 先获取 DNS 服务器的实例标识，再根据 DNS 服务器的实例标识从地址解析器获取 DNS 服务器的地址，以及根据 DNS 服务器的实例标识从 DNS 服务器或其他存储网元或本地获取安全信息；又或者，拜访地的会话管理功能网元先从本地或 NRF 获取 DNS 服务器的实例标识和安全信息，再根据 DNS 服务器的实例标识从地址解析器获取 DNS 服务器的地址。

在又一种可能的实现方式中，拜访地的会话管理功能网元可以根据本地策略，获取安全信息。

可选地，本地策略指示在终端设备支持 DNS over (D)TLS 的情况下，获取安全信息。例如，拜访地的会话管理功能网元接收的第二 PCO 中包含 DNS over (D)TLS，则确定获取安全信息。

可选地，本地策略可以包含每个 DNN/S-NSSAI 支持或允许 HR-SBO 的信息。那么，拜访地的会话管理功能网元可以从本地策略的每个 DNN/S-NSSAI 支持或允许的 HR-SBO 的信息中，确定终端设备请求的 DNN/S-NSSAI 是否支持或允许 HR-SBO，进而选择 DNS 服务器，并获取 DNS 服务器的安全信息和 DNS 服务器的地址。例如，拜访地的会话管理功能网元从本地或 NRF 获取 DNS 服务器的实例标识，安全信息和 DNS 服务器地址；再例如，拜访地的会话管理功能网元从本地或 NRF 先获取 DNS 服务器的实例标识，再根据 DNS 服务器的实例标识从地址解析器获取 DNS 服务器的地址，以及根据 DNS 服务器的实例标识从 DNS 服务器或其他存储网元或本地获取安全信息；又例如，拜访地的会话管理功能网元先从本地或 NRF 获取 DNS 服务器的实例标识和安全信息，再根据 DNS 服务器的实例标识从地址解析器获取 DNS 服务器的地址。

可选地，本地策略还可以包含 PLMN 信息，用于指示可以为哪些 PLMN 的用户提供 HR-SBO 的业务。那么，拜访地的会话管理功能网元可以判断终端设备是否属于该 PLMN，例如终端设备的 HPLMN 是否

为该 PLMN，或者终端设备是否为该 PLMN 的签约用户，若终端设备的 HPLMN 不是该 PLMN，或者终端设备不属于该 PLMN，则拜访地的会话管理功能网元可以跳过 DNS 服务器的发现；若终端设备的 HPLMN 是该 PLMN，或者终端设备属于该 PLMN，则拜访地的会话管理功能网元可以选择支持 HR-SBO 的 DNS 服务器，例如 V-EASDF。

可选地，上述提供的本地策略可以独立实现，也可以组合实现。例如，拜访地的会话管理功能网元可以判断终端设备是否属于该 PLMN，以及判断终端设备请求的 DNN/S-NSSAI 是否支持或允许 HR-SBO，进一步地，只有在确定终端设备属于该 PLMN，且终端设备请求的 DNN/S-NSSAI 支持或允许 HR-SBO 的情况下，拜访地的会话管理功能网元才执行步骤 S302。

在又一种可能的实现方式中，在拜访地的会话管理功能网元获取位于拜访地的 DNS 服务器的安全信息之前，拜访地的会话管理功能网元接收来自归属地的会话管理功能网元的归属地的网络标识。进一步地，拜访地的会话管理功能网元根据终端设备的网络标识，获取安全信息。

示例性的，拜访地的会话管理功能网元可以根据终端设备的 HPLMN 的标识，确定 DNS 服务器的安全信息，该安全信息用于 HPLMN ID 对应的 PLMN 中的签约用户与 DNS 服务器进行安全的消息交互。因此，在该实现方式中，针对不同的 HPLMN，可以确定不同的 DNS 服务器的安全信息。也就是说，对于不同 HPLMN 的终端设备，用于认证 DNS 服务器的安全信息，例如凭证也就不同。

在又一种可能的实现方式中，在拜访地的会话管理功能网元获取位于拜访地的 DNS 服务器的安全信息之前，拜访地的会话管理功能网元接收来自归属地的会话管理功能网元的与会话对应的用户面安全策略。进一步地，拜访地的会话管理功能网元根据用户面安全策略，获取安全信息。

其中，用户面安全策略指示不开启或者可选开启用户面安全保护。在本申请实施例中，用户面安全策略也可以理解为用户面完整性保护策略，二者可替换使用。

示例性的，拜访地的会话管理功能网元在接收到来自归属地的会话管理功能网元的用户面安全策略后，确定该会话对应的用户面安全为不开启或者可选开启用之后，确定 UE 与 DNS 服务器之间需要建立安全连接，以保证两者之间的安全通信。因此，拜访地的会话管理功能网元需要获取 DNS 服务器的安全信息，并通过归属地的会话管理功能网元发送给终端设备，以便于终端设备后续使用安全信息，建立自身与 DNS 服务器之间的安全连接。

可选地，在用户面安全策略指示开启用户面安全的情况下，拜访地的会话管理功能网元也可以获取安全信息，本申请对此不作具体限定。

示例性的，在 PDU 会话的用户面安全策略指示不需要用户面的完整性保护的情况下，拜访地的会话管理功能网元可以确定使用 DNS over (D)TLS，则拜访地的会话管理功能网元可以提供安全信息；或者，若 PDU 会话的用户面安全策略指示需要用户面的完整性保护时，则拜访地的会话管理功能网元可以不提供安全信息。

在又一种可能的实现方式中，在拜访地的会话管理功能网元获取位于拜访地的 DNS 服务器的安全信息之前，拜访地的会话管理功能网元接收来自归属地的会话管理功能网元的 HR-SBO 授权信息。进一步地，拜访地的会话管理功能网元根据 HR-SBO 授权信息，获取安全信息和 DNS 服务器的标识。

可选地，HR-SBO 授权信息可以是用于指示终端设备通过会话访问位于拜访地的 DNS 服务器的信息或指示信息，例如 HR-SBO authorization indication 或者 HR-SBO authorization information，本申请对此不作限定。如果 HR-SBO 授权信息是指示信息，可以直接指示，也可以间接指示，用于判断 HR-SBO 是否授权。

示例性的，拜访地的会话管理功能网元根据 HR-SBO 授权信息，确定在接收到请求 HR-SBO PDU 会话的情况下，需要提供 DNS 服务器的安全信息和 DNS 服务器的标识。

可选地，在确定终端设备满足 HR-SBO 会话建立条件的情况下，拜访地的会话管理功能网元根据 HR-SBO 授权信息，获取安全信息和 DNS 服务器的标识。

示例性的，拜访地的会话管理功能网元可以根据终端设备的位置信息，确定终端设备是否移动待可以接入 V-PLMN 中的边缘应用的区域内。如果确定终端设备当前移动到边缘应用的服务范围，则可以确定满足 HR-SBO 会话建立条件，并且基于本地存储的 HR-SBO 授权信息，获取安全信息和 DNS 服务器的标识。

S303，拜访地的会话管理功能网元向归属地的会话管理功能网元发送安全信息和 DNS 服务器的标识；

对应的，归属地的会话管理功能网元接收来自拜访地的会话管理功能网元的安全信息和 DNS 服务器

的标识。

示例性的，通过 Nsmf_PDUSession_Creat Request 消息发送安全信息和 DNS 服务器的标识。

可选地，拜访地的会话管理功能网元可以分别向归属地的会话管理功能网元发送安全信息和 DNS 服务器的标识。即，拜访地的会话管理功能网元可以通过第一消息向归属地的会话管理功能网元发送 DNS 服务器的标识，通过第二消息向归属地的会话管理功能网元发送安全信息。也就是说，安全信息和 DNS 服务器的标识可以不在同一个消息中发送，也可以不同时发送，本申请实施例对安全信息和 DNS 服务器的标识的发送时机和承载方式不作具体限定。

可选地，拜访地的会话管理功能网元获取策略信息，策略信息用于指示归属地的会话管理功能网元向终端设备发送安全信息的触发条件；进一步地，拜访地的会话管理功能网元还可以向归属地的会话管理功能网元发送策略信息。

示例性的，触发条件可以是：在确定终端设备支持 DNS over (D)TLS 的情况下，归属地的会话管理功能网元可以向终端设备提供安全信息；或者，在确定终端设备支持 DNS over (D)TLS，且 PDU 会话用户面安全策略指示不需要完整性保护或推荐完整性保护的情况下，归属地的会话管理功能网元可以向终端设备提供安全信息等。

S304，归属地的会话管理功能网元生成第一 PCO。

其中，第一 PCO 包括 DNS 服务器的安全信息和 DNS 服务器的标识。

可选地，第一 PCO 还可以包括以下一项或者多项：DNS 服务器支持的一种或者多种安全协议类型中的一个或者多个安全协议类型，建立终端设备与 DNS 服务器之间的安全连接所使用的端口号。

需要指出的是，第一 PCO 中包含的一个或者多个安全协议类型，与上述步骤 S303 中接收到的安全信息中携带的 DNS 服务器支持的一种或者多种安全协议类型，可以相同，也可以不同，本申请对此不作限定。

示例性的，拜访地的会话管理功能网元提供的 DNS 服务器可以支持安全协议 1 和安全协议 2，对应的，拜访地的会话管理功能网元发送的安全信息中包括安全协议 1 和安全协议 2，第一 PCO 中包含的 DNS 服务器支持的安全协议类型可以是安全协议 1 和/或安全协议 2。例如，情况一：第二 PCO 中携带的终端设备支持的安全协议类型是安全协议 1 和安全协议 2，则拜访地的会话管理功能网元确定第一 PCO 中包含安全协议 1 和安全协议 2；或者，情况二：第二 PCO 中携带的终端设备支持的安全协议类型是安全协议 1，则拜访地的会话管理功能网元确定第一 PCO 中包含安全协议 1 等。可选地，针对上述情况二，拜访地的会话管理功能网元发送给终端设备的第一 PCO 中也可以同时包含安全协议 1 和安全协议 2，后续终端设备可以根据自己支持的安全协议类型，例如安全协议 1（适用于 TLS 连接），在确定发起 DNS 发现流程时，根据安全信息与 DNS 服务器建立 TLS 连接，并使用 TLS 连接发送 DNS 消息。

下面针对归属地的会话管理功能网元生成第一 PCO 的具体实现方式进行具体说明。

示例性的，归属地的会话管理功能网元向统一数据管理功能网元发送签约数据管理请求消息；归属地的会话管理功能网元接收来自统一数据管理功能网元的签约数据管理响应消息，其中，签约数据管理响应消息包括归属地路由会话疏导 HR-SBO 授权信息。

在一种可能的实现方式中，归属地的会话管理功能网元生成第一 PCO 根据 HR-SBO 授权信息，生成第一 PCO。示例性的，归属地的会话管理功能网元根据 SDM 信息中携带的 HR-SBO 授权信息，确定 HR-SBO PDU 会话被授权，进一步的根据接收来自拜访地的会话管理功能网元的安全信息生成第一 PCO。

在另一种可能的实现方式中，归属地的会话管理功能网元可以根据本地策略，和/或 PDU 会话的用户面安全策略，确定生成第一 PCO。例如，在该 PDU 会话的用户面安全策略指示不需要用户面的完整性保护的情况下，归属地的会话管理功能网元可以确定第一 PCO 中包含安全信息；再例如，在本地策略指示 PDU 会话的用户面安全策略指示不需要用户面的完整性保护的情况下，归属地的会话管理功能网元确定第一 PCO 中包含安全信息。

在又一种可能的实现方式中，归属地的会话管理功能网元接收来自拜访地的会话管理功能网元的策略信息，策略信息用于指示归属地的会话管理功能网元向终端设备发送安全信息的触发条件；归属地的会话管理功能网元根据策略信息生成第一 PCO。

示例性的，当触发条件为：在确定终端设备支持 DNS over (D)TLS 的情况下，归属地的会话管理功能网元可以向终端设备提供安全信息，则归属地的会话管理功能网元可以根据从拜访地的会话管理功能网元接收到第二 PCO 确定终端设备支持 DNS over (D)TLS，进而可以触发向终端设备提供安全信息。其

中，该第二 PCO 中携带终端设备支持的安全协议为 DNS over (D)TLS。

示例性的，当触发条件为：在确定终端设备支持 DNS over (D)TLS，且 PDU 会话用户面安全策略指示不需要完整性保护或推荐完整性保护的情况下，归属地的会话管理功能网元可以向终端设备提供安全信息，则归属地的会话管理功能网元在根据本地配置的 PDU 会话用户面安全策略确定不需要开启完整性保护的情况下，可以根据从拜访地的会话管理功能网元接收到第二 PCO 确定终端设备支持 DNS over (D)TLS，触发向终端设备提供安全信息等。

在又一种可能的实现方式中，归属地的会话管理功能网元可以根据本地配置信息确定生成第一 PCO。示例性的，归属地的会话管理功能网元获取 H-DNS 服务器，并根据接收来自拜访地的会话管理功能网元的第二 PCO 中包含 DNS 服务器安全信息指示的情况下，确定生成的第一 PCO 中包含对应的 H-DNS 服务器的安全信息；进一步地，归属地的会话管理功能网元向拜访地的会话管理功能网元发送 HR-SBO 授权信息，并接收来自拜访地的会话管理功能网元的用于请求获取安全信息和 DNS 服务器的标识，进而生成第一 PCO。

在又一种可能的实现方式中，归属地的会话管理功能网元接收来自拜访地的会话管理功能网元的第二 PCO 中包含 DNS 服务器安全协议支持，归属地的会话管理功能网元根据 DNS 服务器安全协议支持，生成第一 PCO。

示例性的，归属地的会话管理功能网元可以根据第二 PCO 中携带的终端设备安全协议支持，以及 DNS 服务器支持的一种或者多种安全协议类型，确定生成第一 PCO，第一 PCO 中包括 DNS 服务器和终端设备都支持的一种或者多种安全协议类型中的一个或者多个安全协议类型。

在又一种可能的实现方式中，在归属地的会话管理功能网元生成第一 PCO 之前，归属地的会话管理功能网元接收来自拜访地的会话管理功能网元的第二 PCO，第二 PCO 包括用于指示终端设备支持基于安全协议对 DNS 消息进行安全保护的指示信息；归属地的会话管理功能网元向拜访地的会话管理功能网元发送请求消息，请求消息包括用于指示终端设备支持基于安全协议对 DNS 消息进行安全保护指示信息；归属地的会话管理功能网元接收来自拜访地的会话管理功能网元的安全信息，进而生成第一 PCO。

可选地，归属地的会话管理功能网元可以根据接收来自拜访地的会话管理功能网元的第二 PCO 中携带的用于指示终端设备支持基于安全协议对 DNS 消息进行安全保护的指示信息，确定第一 PCO 中包含安全信息。

可选地，在第二 PCO 还包括终端设备支持的一种或者多种安全协议类型的情况下，归属地的会话管理功能网元根据第二 PCO 中携带的终端设备支持的一种或者多种安全协议类型，以及 DNS 服务器支持的一种或者多种安全协议类型，生成第一 PCO，其中，第一 PCO 包括 DNS 服务器和终端设备都支持的一种或者多种安全协议类型中的一个或者多个安全协议类型。

S305，归属地的会话管理功能网元向拜访地的会话管理功能网元发送第一 PCO；

对应的，拜访地的会话管理功能网元接收来自归属地的会话管理功能网元的第一 PCO。

示例性的，归属地的会话管理功能网元通过 Nsmf_PDUSession_Creat Response 消息向拜访地的会话管理功能网元发送第一 PCO。

在一种示例中，在拜访地的会话管理功能网元接收来自归属地的会话管理功能网元的第一 PCO 之前，拜访地的会话管理功能网元向归属地的会话管理功能网元发送 DNS 服务器支持的一种或者多种安全协议类型，和/或建立安全连接所使用的端口号；其中，第一 PCO 中还包括 DNS 服务器支持的一种或者多种安全协议类型中的一个或者多个安全协议类型和/或端口号。

需要指出的是，拜访地的会话管理功能网元提供的 DNS 服务器支持的一种或者多种安全协议类型，与第一 PCO 中携带的一个或者多个安全协议类型可以完全相同，也可以不同，本申请对此不作限定。例如，拜访地的会话管理功能网元提供的 DNS 服务器支持的安全协议为安全协议 1 和安全协议 2，归属地的会话管理功能网元向终端设备提供的第一 PCO 中可以包含安全协议 1 和/或安全协议 2。

S306，拜访地的会话管理功能网元向终端设备发送第一 PCO；

对应的，终端设备接收来自拜访地的会话管理功能网元的第一 PCO。

示例性的，拜访地的会话管理功能网元（例如 V-SMF）向移动管理功能网元（例如 AMF）发送 PDU session Establishment Response 消息发送第一 PCO，AMF 通过 Nsmf_PDUSession_CreatSMContext Response 消息向终端设备（例如 UE）发送第一 PDU 会话建立响应消息。例如，V-SMF 向 AMF 发送第一 PCO。

S307，终端设备基于安全信息，建立与DNS服务器（例如V-EASDF）之间的安全连接。

示例性的，终端设备在接收到 DNS 服务器的安全信息后，终端设备将安全信息传递到上层。进一步地，在 UE 确定发起 DNS 发现流程时，终端设备使用该安全信息建立与 DNS 服务器之间的(D)TLS 安全连接，并使用建立的(D)TLS 安全连接发送 DNS 消息。应理解，该 DNS 消息是被保护的，可以保证终端设备与 DNS 服务器之间的安全通信。

可选地，在上述提供的本申请技术方案中，归属地的会话管理功能网元获取 DNS 服务器（例如，V-EASDF）的安全信息的实现方式还可以包括：

示例性的，在归属地的会话管理功能网元中预配置位于拜访地的 DNS 服务器的安全信息，例如预配置中包含 V-PLMN ID1，以及关联的 V-EASDF 的安全信息；又例如 V-PLMN ID2，以及关联的 V-EASDF 的安全信息等。针对同一个 V-PLMN，不同的 V-EASDF 的安全信息可以是相同的，也可以是不同的。当不同的 V-EASDF 的安全信息相同时，预配置中仅需要包含 V-PLMN ID 和关联的 V-EASDF 的安全信息。当安全信息不同时，预配置中同时还需要存储 V-EASDF 的 ID。在确定归属地路由本地疏导（home routed local breakout，HR-LBO）授权的情况下，归属地的会话管理功能网元可以根据接收到的 DNS 服务器地址，用于指示终端设备支持基于安全协议对 DNS 消息进行安全保护的指示信息，VPLMN ID，DNS 服务器支持的安全协议类型，确定在第一 ePCO 中包含 V-EASDF 的安全信息。

示例性的，在 UDM 中预配置位于拜访地的 DNS 服务器（例如，V-EASDF）的安全信息，例如 V-PLMN ID1，以及关联的 V-EASDF 的安全信息；又例如 V-PLMN ID2，以及关联的 V-EASDF 的安全信息等。在确定 HR-LBO 授权的情况下，归属地的会话管理功能网元可以根据接收到的拜访网络的 V-PLMN ID 和/或 V-EASDF 地址，从 UDM 获取 V-EASDF 的安全信息。其中，针对同一个 V-PLMN，不同的 V-EASDF 的安全信息可以是相同的，也可以是不同的，具体实现可参考上述相关描述。

应理解，上述获取 DNS 服务器的安全信息的替换方法与方法 300 的区别在于，该可选的实现方式中归属地的会话管理功能网元不与归属地的会话管理功能网元进行信息交互，自己从本地的预配置或者从 UDM 获取 DNS 服务器的安全信息。另外，该实现方式同样适应于以下方法 400 至 800 中，为了简洁，下文不再重复赘述。

本申请提供的方案，通过拜访地的会话管理功能网元与归属地的会话管理功能网元交互安全信息，再由归属地的会话管理功能网元将安全信息发送给终端设备，使得终端设备可以根据安全信息建立与 DNS 服务器之间的安全连接，从而保障网络通信安全。

接下来，以终端设备为 UE，拜访地边缘应用服务器发现功能网元为 V-EASDF，拜访地的会话管理功能网元为 V-SMF，归属地的会话管理功能网元为 H-SMF，移动管理功能网元为 AMF，统一数据管理功能网元为 UDM 为例，结合图 4 至图 8，分别说明 UE 与 V-EASDF 之间建立安全连接的方案。

图 4 是本申请实施例提供的通信方法 400 的流程示例图。该方法在 HR-SBO PDU 会话建立过程中，V-SMF 在确定发起 HR-SBO PDU 会话的情况下，向 H-SMF 同时提供 V-EASDF 地址和 V-EASDF 的安全信息#a，进而使得 H-SMF 能够确定向 UE 发送 V-EASDF 的安全信息#b，能够节省信令开销。如图 4 所示，该方法包括如下多个步骤。

S401，UE 注册流程，AMF 从 UDM 获取 HR-SBO 允许指示。

其中，注册流程的具体实现方式可参考上述方法 200 的步骤 S201 至 S204 的相关描述，为了简洁，此处不再赘述。

S402，UE 向 AMF 发送 PDU 会话建立请求#a；对应的，AMF 接收来自 UE 的 PDU 会话建立请求#a。

示例性的，若 UE 支持 DNS over (D)TLS，则 PDU 会话建立请求#a 中包含 ePCO#a，ePCO#a 包含 DNS 服务器安全信息指示。可选地，ePCO#a 还可以包含 DNS 服务器安全协议支持，用于指示 UE 支持的安全协议类型。

S403，AMF 选择 V-SMF。

S404，AMF 向 V-SMF 发送创建会话管理上下文请求；对应的，V-SMF 接收来自 AMF 的创建会话管理上下文请求。

S405，V-SMF 向 AMF 发送创建会话管理上下文响应；对应的，AMF 接收来自 V-SMF 的创建会话管理上下文响应。

其中，上述步骤 S402 至 S405 的具体实现方式，以及交互消息的具体名称或含义，可参考上述方法 200 的步骤 S205 至 S207 的相关描述，为了简洁，此处不再过多赘述。

S406，V-SMF 获取 V-EASDF 的安全信息#a。

其中，安全信息#a 可以包括认证凭证，用于认证 V-EASDF 的凭证。可选地，安全信息#a 还可以包括 V-EASDF 支持的安全协议信息（或者说，V-EASDF 支持的安全机制），和/或端口号等。

在一种示例中，若步骤 S404 中包含 HR-SBO 允许指示，则 V-SMF 选择支持 HR-SBO 的 V-EASDF，并获取 V-EASDF 的安全信息#a 和 V-EASDF 的地址。例如，V-SMF 从本地或 NRF 获取 V-EASDF 实例标识，V-EASDF 地址和安全信息#a；再例如，V-SMF 从本地或 NRF 先获取 V-EASDF 实例标识，再根据 V-EASDF 实例标识从地址解析器获取 V-EASDF 地址，以及根据 V-EASDF 实例标识从 V-EASDF 或其他存储网元或本地获取安全信息#a；又例如，V-SMF 先从本地或 NRF 获取 V-EASDF 实例标识和安全信息#a，再根据 V-EASDF 实例标识从地址解析器获取 V-EASDF 的地址。

在另一种示例中，若步骤 S404 中不包含 HR-SBO 允许指示，则 V-SMF 可以根据本地策略确定选择 V-EASDF，并获取 V-EASDF 的安全信息#a 和 V-EASDF 的地址。

示例性的，本地策略包含 per DNN/S-NSSAI 支持或允许 HR-SBO 的信息。那么，V-SMF 可以从本地策略的 per DNN/S-NSSAI 支持或允许的 HR-SBO 的信息中，确定与步骤 S402 的 PDU 会话建立请求#a 中携带的 DNN/S-NSSAI 是否支持或允许 HR-SBO，进而选择 V-EASDF，并获取 V-EASDF 的安全信息#a 和 V-EASDF 的地址。例如，V-SMF 从本地或 NRF 获取 V-EASDF 实例标识，V-EASDF 地址和安全信息#a；再例如，V-SMF 从本地或 NRF 先获取 V-EASDF 实例标识，再根据 V-EASDF 实例标识从地上解析器获取 V-EASDF 地址，以及根据 V-EASDF 实例标识从 V-EASDF 或其他存储网元或本地获取安全信息#a；又例如，V-SMF 先从本地或 NRF 获取 V-EASDF 实例标识和安全信息#a，再根据 V-EASDF 实例标识从地址解析器获取 V-EASDF 的地址。

可选地，本地策略还可以包含 PLMN 信息，用于指示可以为哪些 PLMN 的用户提供 HR-SBO 的业务。那么，V-SMF 可以判断 UE 是否属于该 PLMN，即 UE 的 HPLMN 是否为该 PLMN 或 UE 为该 PLMN 的签约用户，若 UE 不属于该 PLMN，则 V-SMF 跳过 V-EASDF 的发现；若 UE 属于该 PLMN，则 V-SMF 选择支持 HR-SBO 的 V-EASDF。

可选地，上述提供的本地策略可以独立实现，也可以组合实现。例如，V-SMF 需要判断 UE 是否属于该 PLMN，以及判断 UE 请求的 DNN/S-NSSAI 是否支持或允许 HR-SBO，只有在确定 UE 属于该 PLMN，且 UE 请求的 DNN/S-NSSAI 支持或允许 HR-SBO 的情况下，V-SMF 才执行步骤 S406。

可选地，在上述示例中，V-SMF 可以根据 UE 的 HPLMN 的标识，确定 V-EASDF 的安全信息#a。因此，在该实现方式中，针对不同的 HPLMN，可以确定不同的 V-EASDF 的安全信息。也就是说，对于不同 HPLMN 的 UE，用于认证 V-EASDF 的凭证也就不同。

可选地，V-SMF 还可以获取策略信息#a，携带在步骤 S407 中发送给 H-SMF，用于 H-SMF 确定是否向 UE 提供 V-EASDF 的安全信息#a。例如，策略信息#a 指示在 UE 支持 DNS over (D)TLS 的情况下，则 H-SMF 可以向 UE 提供 V-EASDF 的安全信息；又例如，策略信息#a 指示在 UE 支持 DNS over (D)TLS，且 PDU 会话用户面安全策略指示不需要完整性保护的情况下，则 H-SMF 可以向 UE 提供 V-EASDF 的安全信息等。应理解，上述策略信息#a 仅是为便于理解方案给出的示例，本申请实施例对策略信息#a 不作具体限定。

S407，V-SMF 向 H-SMF 发送 PDU 会话建立请求#b；对应的，H-SMF 接收来自 V-SMF 的 PDU 会话建立请求#b。

其中，PDU 会话建立请求#b 包括 ePCO#a、V-EASDF 的安全信息#a 和 V-EASDF 的地址。

可选地，如果步骤 S406 中 V-SMF 获取了策略信息#a，则 PDU 会话建立请求#b 可以携带该策略信息#a。

S408，H-SMF 向 UDM 请求获取 SDM 信息；对应的，UDM 接收来自 H-SMF 的获取 SDM 信息的请求。

S409，UDM 向 H-SMF 发送 SDM 信息；对应的，H-SMF 接收来自 UDM 的 SDM 信息。

其中，上述步骤 S408 和 S409 的具体实现方式，以及交互消息的具体名称或含义，可参考上述方法 200 的步骤 S209 和 S210 的相关描述，为了简洁，此处不再过多赘述。

S410，H-SMF 在确定 HR-SBO 授权的情况下，确定 V-EASDF 的安全信息#b（即，安全信息的一例）。

其中，安全信息#b 可以包括认证凭证，即用于认证 V-EASDF 的凭证。可选地，安全信息#b 还可以

包括 V-EASDF 支持的安全协议信息（或者说，V-EASDF 支持的安全机制），和/或端口号等。

示例性的，H-SMF 根据步骤 S409 的 SDM 信息中携带的 HR-SBO 授权指示和/或 HR-SBO 授权信息，确定 HR-SBO PDU 会话被授权。

进一步地，H-SMF 确定生成包含 V-EASDF 的安全信息#b 的 ePCO#b。另外，ePCO#b 中还包含 V-EASDF 的地址。

在一种示例中，H-SMF 可以根据在步骤 S407 接收到的 ePCO#a 中包含 DNS 服务器安全信息指示，确定在 ePCO#b 中包含 V-EASDF 的安全信息#b。

在另一种示例中，H-SMF 可以根据本地策略，和/或 PDU 会话的用户面安全策略，确定在 ePCO#b 中包含 V-EASDF 的安全信息#b。例如，在该 PDU 会话的用户面安全策略指示不需要用户面的完整性保护的情况下，H-SMF 确定 ePCO#b 中包含 V-EASDF 的安全信息#b；再例如，在本地策略指示 PDU 会话的用户面安全策略指示不需要用户面的完整性保护的情况下，H-SMF 确定 ePCO#b 中包含 V-EASDF 的安全信息#b。

在又一种示例中，如果上述步骤 S407 的 PDU 会话建立请求#b 中携带了策略信息#a，则 H-SMF 还可以根据该策略信息#a 确定 ePCO#b 中包含 V-EASDF 的安全信息#b。例如，策略信息#a 指示在 UE 支持 DNS over(D)TLS 的情况下，使用 DNS over (D)TLS，无需考虑 PDU 会话的用户面安全策略，则在确定 HR-SBO 授权，且来自 UE 的 ePCO#a 中包含 DNS 服务器安全信息指示的情况下，H-SMF 可以确定在 ePCO#b 中包含 V-EASDF 的安全信息#b。又例如，策略信息#a 指示在 PDU 会话的用户面安全策略指示不需要用户面的完整性保护时，使用 DNS over (D)TLS，则 H-SMF 可以确定 ePCO#b 中包含 V-EASDF 的安全信息#b。

在又一种示例中，如果在步骤 S407 接收到的 ePCO#a 中包含 DNS 服务器安全协议支持，则 H-SMF 可以根据 ePCO#a 中携带的 DNS 服务器安全协议支持，以及步骤 S407 接收到的 V-EASDF 的安全信息#a 中携带的安全协议信息，确定最终使用的安全协议，并将该 DNS 服务器安全协议作为 V-EASDF 的安全信息#b 的一部分携带在 ePCO#b 中。

应理解，以上仅是为便于理解给出的示例，不应构成对本申请技术方案的任何限定。

可选地，V-EASDF 的安全信息#b 与 V-EASDF 的安全信息#a 可以相同，也可以不同。具体来说，V-EASDF 的安全信息#b 包含于 V-EASDF 的安全信息#a，或者说 V-EASDF 的安全信息#b 是 V-EASDF 的安全信息#a 的子集。例如，V-EASDF 的安全信息#b 包含凭证 1，安全协议 1，V-EASDF 的安全信息#a 包含凭证 1，安全协议 1 和安全协议 2。

S411，H-SMF 向 V-SMF 发送 PDU 会话建立响应#b；对应的，V-SMF 接收来自 H-SMF 的 PDU 会话建立响应#b。

其中，PDU 会话建立响应#b 包括 ePCO#b，ePCO#b 包括 V-EASDF 的安全信息#b 和 V-EASDF 的地址。

可选地，PDU 会话建立响应#b 还可以包含 HPLMN 的 DNS 服务器的地址（可以简称为 H-DNS 服务器的地址），该 H-DNS 服务器用于解析特定应用（例如由 HPLMN 能够路由的）的地址。

S412，V-SMF 向 AMF 发送 N1N2 消息传输；对应的，AMF 接收来自 V-SMF 的 N1N2 消息传输。

其中，N1N2 消息传输可以是 N1N2_MessageTransfer，该消息包含 N1 SM 容器，N1 SM 容器包括 ePCO#b，ePCO#b 包括 V-EASDF 的安全信息#b 和 V-EASDF 的地址。

S413，AMF 向 UE 发送 PDU 会话建立响应#a；对应的，UE 接收来自 AMF 的 PDU 会话建立响应#a。

其中，PDU 会话建立响应#a 包括 N1 SM 容器，也就是向 UE 提供 V-EASDF 的安全信息#b 和 V-EASDF 的地址。

S414，PDU 会话建立后续过程。

其中，PDU 会话建立的具体实现方式可参考 3GPP TS23.502 中的相关描述，为了简洁，此处不再赘述。

S415，UE 使用 V-EASDF 的安全信息#b，向 V-EASDF 发送具有安全保护的 DNS 消息；对应的，V-EASDF 接收来自 UE 的具有安全保护的 DNS 消息。

示例性的，UE 接收 V-EASDF 的安全信息#b，UE 将安全信息#b 传递到上层。进一步地，UE 使用该 V-EASDF 的安全信息#b 建立与 V-EASDF 之间的安全连接，并使用建立的安全连接发送 DNS 消息。

示例性的，在 UE 确定发起 DNS 发现流程时，UE 可以根据接收到的 V-EASDF 的安全信息#b 建立

（D）TLS 连接，并使用（D）TLS 连接发送 DNS 消息。应理解，该 DNS 消息是被保护的，可以保证 UE 与 V-EASDF 之间的安全通信。

本申请所揭示的方法，V-SMF 根据来自 AMF 的 HR-SBO 允许指示或本地策略，确定发起 HR-SBO 的 PDU 会话建立过程中，选择 V-EASDF，获取 V-EASDF 的安全信息#a，并向 H-SMF 同时发送该 V-EASDF 的地址和 V-EASDF 的安全信息#a；H-SMF 在确定请求的 HR-SBO PDU 会话授权通过的情况下，能够根据来自 UE 的 ePCO#a 中的 DNS 服务器安全信息指示和来自 V-SMF 的 V-EASDF 的安全信息#a，确定向 UE 发送包含 V-EASDF 的安全信息#b 的 ePCO#b。基于该实现方式，能够保护 V-EASDF 与 UE 之间交互的 DNS 消息，维护网络安全通信。

图 5 是本申请实施例提供的通信方法 500 的流程示例图。该方法在 HR-SBO PDU 会话建立过程中，由 H-SMF 主动触发向 V-SMF 获取 V-EASDF 的安全信息#a，使得网络能够按需获取安全信息#a，即 V-SMF 根据 H-SMF 的请求向 H-SMF 提供 V-EASDF 的安全信息#a，进而使得 H-SMF 能够确定向 UE 发送 V-EASDF 的安全信息#b。如图 5 所示，该方法包括如下多个步骤。

S501，UE 注册流程，AMF 从 UDM 获取 HR-SBO 允许指示。

S502，UE 向 AMF 发送 PDU 会话建立请求#A；对应的，AMF 接收来自 UE 的 PDU 会话建立请求#A。

示例性的，若 UE 支持 DNS over (D)TLS，则 PDU 会话建立请求#A 中包含 ePCO#A，ePCO#A 包含 DNS 服务器安全信息指示。可选地，ePCO#A 还可以包含 DNS 服务器安全协议支持。

S503，AMF 选择 V-SMF。

S504，AMF 向 V-SMF 发送创建会话管理上下文请求；对应的，V-SMF 接收来自 AMF 的创建会话管理上下文请求。

S505，V-SMF 向 AMF 发送创建会话管理上下文响应；对应的，AMF 接收来自 V-SMF 的创建会话管理上下文响应。

其中，上述步骤 S501 至 S505 的具体实现方式，以及交互消息的具体名称或含义，可参考上述方法 400 的步骤 S401 至 S405 的相关描述，为了简洁，此处不再过多赘述。

S506，V-SMF 获取 V-EASDF 的地址。

在一种示例中，若步骤 S504 中包含 HR-SBO 允许指示，则 V-SMF 选择支持 HR-SBO 的 V-EASDF，并获取 V-EASDF 的地址。

在另一种示例中，若步骤 S504 中不包含 HR-SBO 允许指示，则 V-SMF 可以根据本地策略确定选择 V-EASDF，并获取 V-EASDF 的地址。

示例性的，本地策略包含 per DNN/S-NSSAI 支持或允许 HR-SBO 的信息。可选地，本地策略还可以包含 PLMN 信息，用于指示可以为哪些 PLMN 的用户提供 HR-SBO 的业务。具体实现方式可参考上述方法 400 的步骤 S406 的相关描述，为了简洁，此处不再过多赘述。

S507，V-SMF 向 H-SMF 发送 PDU 会话建立请求#B；对应的，H-SMF 接收来自 V-SMF 的 PDU 会话建立请求#B。

其中，PDU 会话建立请求#B 包括 ePCO#A 和 V-EASDF 的地址。

S508，H-SMF 向 UDM 请求获取 SDM 信息；对应的，UDM 接收来自 H-SMF 的获取 SDM 信息的请求。

S509，UDM 向 H-SMF 发送 SDM 信息；对应的，H-SMF 接收来自 UDM 的 SDM 信息。

其中，上述步骤 S508 和 S509 的具体实现方式，以及交互消息的具体名称或含义，可参考上述方法 400 的步骤 S408 和 S409 的相关描述，为了简洁，此处不再过多赘述。

S510，H-SMF 在确定 HR-SBO 授权的情况下，触发 V-EASDF 的安全信息的获取流程。

示例性的，H-SMF 根据步骤 S509 的 SDM 信息中携带的 HR-SBO 授权指示和/或 HR-SBO 授权信息，确定 HR-SBO PDU 会话被授权；同时，若在步骤 S507 接收到的 ePCO#A 中携带 DNS 服务器安全信息指示，则 H-SMF 触发向 V-SMF 获取 V-EASDF 的安全信息#a，即执行步骤 S511 至 S513。

可选地，H-SMF 可以在接收到来自 V-SMF 的 V-EASDF 地址的情况下，执行步骤 S511 至 S513。

S511。H-SMF 向 V-SMF 发送安全信息请求；对应的，V-SMF 接收来自 H-SMF 的安全信息请求。

示例性的，安全信息请求可以是 Nsmf_Info Request，即消息本身可以指示 H-SMF 请求从 V-SMF 获取 V-EASDF 的安全信息#a。

可选地，安全信息请求中包含以下一项或者多项：DNS 服务器安全信息指示，PDU 会话的用户面安

全策略，HPLMN ID，DNS服务器安全协议支持。

S512，V-SMF确定是否提供V-EASDF的安全信息#a。

在一种示例中，V-SMF根据步骤S511中接收到的安全信息请求确定使用DNS over (D)TLS，则在步骤S513的安全信息响应中携带V-EASDF的安全信息#a。

在另一种示例中，若步骤S511的安全信息请求中包含DNS服务器安全信息指示，则V-SMF可以根据DNS服务器安全信息指示，确定使用DNS over (D)TLS，并在步骤S513的安全信息响应中携带V-EASDF的安全信息#a。

在又一种示例中，V-SMF可以根据本地策略确定是否提供V-EASDF的安全信息#a。例如，本地策略指示在UE支持DNS over (D)TLS的情况下，则V-SMF可以根据S507中携带的ePCO#A包含的DNS over (D)TLS，确定在步骤S513的安全信息响应中携带V-EASDF的安全信息#a。

在又一种示例中，若步骤S511的安全信息请求中包含PDU会话的用户面安全策略，则V-SMF可以根据PDU会话的用户面安全策略，确定是否提供V-EASDF的安全信息#a。例如，在PDU会话的用户面安全策略指示不需要用户面的完整性保护的情况下，V-SMF可以确定使用DNS over (D)TLS，并在步骤S513的安全信息响应中携带V-EASDF的安全信息#a；或者，若PDU会话的用户面安全策略指示需要用户面的完整性保护时，则V-SMF可以不提供V-EASDF的安全信息#a。

在又一种示例中，若步骤S511的安全信息请求中包含HPLMN ID，则V-SMF可以根据HPLMN ID提供V-EASDF的安全信息#a。例如，获取HPLMN ID对应的V-EASDF的安全信息#a，该安全信息#a用于HPLMN ID对应的PLMN中的签约用户与V-EASDF安全的交互消息。

在又一种示例中，若步骤S511的安全信息请求中包含DNS服务器安全协议支持，则V-SMF可以根据DNS服务器安全协议支持，确定提供V-EASDF的安全信息#a。

需要说明的是，上述提供的示例可以独立实现，也可以组合实现。示例性的，V-SMF可以根据本地策略，以及PDU会话的用户面安全策略，是否提供V-EASDF的安全信息#a。例如，本地策略指示只有在PDU会话的用户面安全策略指示不需要用户面的完整性保护的情况下，V-SMF可以提供V-EASDF的安全信息#a。示例性的，V-SMF可以根据本地策略和HPLMN ID，确定是否提供V-EASDF的安全信息#a。例如，本地策略指示在UE支持DNS over (D)TLS，且UE属于该HPLMN的情况下，V-SMF可以提供对应PLMN中的用户与V-EASDF安全交互的安全信息#a，等等。

应理解，以上仅是为便于理解给出的示例，不应构成对本申请技术方案的任何限定。

S513，V-SMF向H-SMF发送安全信息响应；对应的，H-SMF接收来自V-SMF的安全信息响应。

其中，安全信息响应中携带V-EASDF的安全信息#a。

示例性的，基于步骤S512的判断，若确定需要提供V-EASDF的安全信息#a，则V-SMF向H-SMF发送Nsmf_Info响应，该Nsmf_Info响应中包含V-EASDF的安全信息#a。

S514，H-SMF向V-SMF发送PDU会话建立响应#B；对应的，V-SMF接收来自H-SMF的PDU会话建立响应#B。

S515，V-SMF向AMF发送N1N2消息传输；对应的，AMF接收来自V-SMF的N1N2消息传输。

S516，AMF向UE发送PDU会话建立响应#A；对应的，UE接收来自AMF的PDU会话建立响应#A。

S517，PDU会话建立后续过程。

S518，UE使用V-EASDF的安全信息#b，向V-EASDF发送具有安全保护的DNS消息；对应的，V-EASDF接收来自UE的具有安全保护的DNS消息。

示例性的，UE接收V-EASDF的安全信息#b，UE将安全信息#b传递到上层。进一步地，UE使用该V-EASDF的安全信息#b建立与V-EASDF之间的安全连接，并使用建立的安全连接发送DNS消息。

其中，上述步骤S514至S518的具体实现方式，以及交互消息的具体名称，可参考上述方法400的步骤S411至S415的相关描述，为了简洁，此处不再过多赘述。

本申请所揭示的方法，在HR-SBO的PDU会话建立过程中，H-SMF在接收到来自UE的DNS服务器安全信息指示，以及确定请求的HR-SBO PDU会话授权通过的情况下，向V-SMF请求获取V-EASDF的安全信息#a，V-SMF根据来自H-SMF的请求消息，和/或本地策略，PDU会话的用户面安全策略，确定向H-SMF发送V-EASDF的安全信息#a，从而使得H-SMF能够向UE发送包含V-EASDF的安全信息#b的ePCO#B。基于该实现方式，能够保护V-EASDF与UE之间交互的DNS消息，维护网络安全通信。

图6是本申请实施例提供的通信方法600的流程示例图。该方法在HR-SBO PDU会话建立过程中，

V-SMF 在接收到来自 H-SMF 的 HR-SBO 授权指示，确定发起 HR-SBO PDU 会话的情况下，向 H-SMF 提供 V-EASDF 的安全信息#a，进而使得 H-SMF 能够确定向 UE 发送 V-EASDF 的安全信息#b。基于 HR-SBO 授权指示获取安全信息#a 能够保障后续 UE 与 V-EASDF 之间的安全通信。如图 6 所示，该方法包括如下多个步骤。

S601，UE 注册流程，AMF 从 UDM 获取 HR-SBO 允许指示。

S602，UE 向 AMF 发送 PDU 会话建立请求#11；对应的，AMF 接收来自 UE 的 PDU 会话建立请求#11。

S603，AMF 选择 V-SMF。

S604，AMF 向 V-SMF 发送创建会话管理上下文请求；对应的，V-SMF 接收来自 AMF 的创建会话管理上下文请求。

S605，V-SMF 向 AMF 发送创建会话管理上下文响应；对应的，AMF 接收来自 V-SMF 的创建会话管理上下文响应。

其中，上述步骤 S601 至 S605 的具体实现方式，以及交互消息的具体名称或含义，可参考上述方法 400 的步骤 S401 至 S405 的相关描述，为了简洁，此处不再过多赘述。

S606，V-SMF 向 H-SMF 发送 PDU 会话建立请求#22；对应的，H-SMF 接收来自 V-SMF 的 PDU 会话建立请求#22。

其中，PDU 会话建立请求#22 包括 ePCO#11。

S607，H-SMF 向 UDM 请求获取 SDM 信息；对应的，UDM 接收来自 H-SMF 的获取 SDM 信息的请求。

S608，UDM 向 H-SMF 发送 SDM 信息；对应的，H-SMF 接收来自 UDM 的 SDM 信息。

其中，上述步骤 S601 至 S608 的具体实现方式，以及交互消息的具体名称或含义，可参考上述方法 400 的步骤 S401 至 S405、S407 至 S409 的相关描述，为了简洁，此处不再过多赘述。

S609，H-SMF 生成 ePCO#22。

示例性的，H-SMF 根据步骤 S608 的 SDM 信息中携带的 HR-SBO 授权指示和/或 HR-SBO 授权信息，确定 HR-SBO PDU 会话被授权，并进一步地生成 ePCO#22。其中，ePCO#22 中包含 H-DNS 服务器的安全信息和 H-DNS 服务器的地址。

在一种示例中，H-SMF 可以根据本地配置信息获取 H-DNS 服务器，在步骤 S606 的 ePCO#11 中包含 DNS 服务器安全信息指示的情况下，确定在 ePCO#22 中包含对应的 H-DNS 服务器的安全信息。

在另一种示例中，H-SMF 可以根据本地策略，和/或 PDU 会话的用户面安全策略，确定在 ePCO#22 中包含对应的 H-DNS 服务器的安全信息。

在又一种示例中，如果上述步骤 S606 的 PDU 会话建立请求#22 中携带了策略信息#a，则 H-SMF 还可以根据该策略信息#a 确定 ePCO#22 中包含包含对应的 H-DNS 服务器的安全信息。

在又一种示例中，如果在步骤 S606 的 PDU 会话建立请求#22 中携带的 ePCO#11 包含 DNS 服务器安全协议支持，则 H-SMF 可以根据 ePCO#11 中携带的 DNS 服务器安全协议支持，确定将该 DNS 服务器安全协议作为 H-DNS 服务器的安全信息的一部分携带在 ePCO#22 中。

应理解，以上仅是为便于理解给出的示例，不应构成对本申请技术方案的任何限定。具体的判断逻辑和实现方式可参考上述方法 400 的步骤 S410 的相关描述，为了简洁，此处不再赘述。

S610，H-SMF 向 V-SMF 发送 PDU 会话建立响应#22；对应的，V-SMF 接收来自 H-SMF 的 PDU 会话建立响应#22。

其中，PDU 会话建立响应#22 包括 ePCO#22。

可选地，若 H-SMF 根据步骤 S608 中的 SDM 信息确定 HR-SBO 被授权，则 PDU 会话建立响应#22 中还可以包含 HR-SBO 授权指示或 HR-SBO 授权信息；若 H-SMF 在步骤 S606 接收到的 ePCO#11 中包含 DNS 服务器安全信息指示，和/或 DNS 服务器安全协议支持，则 PDU 会话建立响应#22 中还可以包含 DNS 服务器安全信息指示，和/或 DNS 服务器安全协议支持。

可选地，PDU 会话建立响应#22 还可以包括 PDU 会话的用户面安全策略。

S611，V-SMF 确定是否提供 V-EASDF 的安全信息#a。

其中，具体的判断逻辑和实现方式可参考上述方法 500 的步骤 S512 的相关描述，为了简洁，此处不再赘述。

S612，V-SMF 向 H-SMF 发送 PDU 会话更新请求；对应的，H-SMF 接收来自 V-SMF 的 PDU 会话更新请求。

示例性的，PDU 会话更新请求可以是 Nsmf_PDUSession_update 请求。其中，PDU 会话更新请求包括 V-EASDF 的安全信息#a 和 V-EASDF 的地址，V-SMF 获取 V-EASDF 的地址的具体实现方式可参考上述方法 500 的步骤 S506 的相关描述，为了简洁，此处不再赘述。

S613，H-SMF 生成 ePCO#33。

其中，ePCO#33 中包含 V-EASDF 的地址和 V-EASDF 的安全信息#b。

需要指出的是，若上述步骤 S610 的 PDU 会话建立响应#22 中不包含 DNS 服务器安全信息指示，则可以由 H-SMF 根据在步骤 S606 接收到的 ePCO#11 中携带的 DNS 服务器安全信息指示，确定向 UE 发送的 V-EASDF 的安全信息#b。进一步地，若步骤 S606 接收到的 ePCO#11 中携带了 DNS 服务器安全协议支持，则 H-SMF 可以根据该 DNS 服务器安全协议支持，确定向 UE 发送的 V-EASDF 的安全信息#b。

S614，H-SMF 向 V-SMF 发送 PDU 会话更新响应；对应的，V-SMF 接收来自 H-SMF 的 PDU 会话更新响应。

示例性的，PDU 会话更新响应可以是 Nsmf_PDUSession_update。其中，PDU 会话更新响应包括 ePCO#33。

可选地，上述步骤 S612 和 S614 的名称仅是为便于理解给出的示例，不应构成对本申请的任何限定。也就是说，PDU 会话更新请求消息和 PDU 会话更新响应消息还可以替换为其他的服务消息。

S615，V-SMF 向 AMF 发送 N1N2 消息传输；对应的，AMF 接收来自 V-SMF 的 N1N2 消息传输。

S616，AMF 向 UE 发送 PDU 会话建立响应#11；对应的，UE 接收来自 AMF 的 PDU 会话建立响应#11。

S617，PDU 会话建立后续过程。

S618，UE 使用 V-EASDF 的安全信息#b，向 V-EASDF 发送具有安全保护的 DNS 消息；对应的，V-EASDF 接收来自 UE 的具有安全保护的 DNS 消息。

其中，上述步骤 S615 至 S618 的具体实现方式，以及交互消息的具体名称，可参考上述方法 400 的步骤 S412 和 S415 的相关描述，为了简洁，此处不再过多赘述。

本申请所揭示的方法，V-SMF 根据来自 H-SMF 的 HR-SBO 授权指示，在确定发起 HR-SBO PDU 会话时，V-SMF 向 H-SMF 发送 V-EASDF 的地址和 V-EASDF 的安全信息#a，使得 H-SMF 能够向 UE 发送包含 V-EASDF 的安全信息#b 的 ePCO#33。基于该实现方式，能够保护 V-EASDF 与 UE 之间交互的 DNS 消息，维护网络安全通信。

图 7 是本申请实施例提供的通信方法 700 的流程示例图。该方法在 HR-SBO PDU 会话建立过程中，H-SMF 确认 HR-SBO 授权时向 V-SMF 发起通知流程，以使得 V-SMF 在确定请求 HR-SBO 的情况下提供 V-EASDF 安全信息#a，进而使得 H-SMF 能够确定向 UE 发送 V-EASDF 的安全信息#b。如图 7 所示，该方法包括如下多个步骤。

S701，UE 注册流程，AMF 从 UDM 获取 HR-SBO 允许指示。

S702，UE 向 AMF 发送 PDU 会话建立请求#α；对应的，AMF 接收来自 UE 的 PDU 会话建立请求#α。

S703，AMF 选择 V-SMF。

S704，AMF 向 V-SMF 发送创建会话管理上下文请求；对应的，V-SMF 接收来自 AMF 的创建会话管理上下文请求。

S705，V-SMF 向 AMF 发送创建会话管理上下文响应；对应的，AMF 接收来自 V-SMF 的创建会话管理上下文响应。

S706，V-SMF 向 H-SMF 发送 PDU 会话建立请求#β；对应的，H-SMF 接收来自 V-SMF 的 PDU 会话建立请求#β。

S707，H-SMF 向 UDM 请求获取 SDM 信息；对应的，UDM 接收来自 H-SMF 的获取 SDM 信息的请求。

S708，UDM 向 H-SMF 发送 SDM 信息；对应的，H-SMF 接收来自 UDM 的 SDM 信息。

其中，上述步骤 S701 至 S708 的具体实现方式，以及交互消息的具体名称或含义，可参考上述方法 600 的步骤 S601 至 S608 的相关描述，为了简洁，此处不再过多赘述。

S709，H-SMF 在确定 HR-SBO 授权的情况下，触发通知流程。

示例性的，H-SMF 根据步骤 S708 的 SDM 信息中携带的 HR-SBO 授权指示和/或 HR-SBO 授权信息，确定 HR-SBO PDU 会话被授权，然后即可执行步骤 S710。

S710，H-SMF 向 V-SMF 发送授权通知消息；对应的，V-SMF 接收来自 H-SMF 的授权通知消息。

示例性的，授权通知消息可以是 Nsmf_info_notify 消息。其中，该授权通知消息中包含 HR-SBO 授权指示或 HR-SBO 授权信息。

可选地，若 H-SMF 在步骤 S706 接收到的 ePCO#α 中包含 DNS 服务器安全信息指示，则该授权通知消息中可以包含 DNS 服务器安全信息指示；若 ePCO#α 中包含 DNS 服务器安全协议支持，则该授权通知消息中可以包含 DNS 服务器安全协议支持。

S711，V-SMF 确定是否提供 V-EASDF 的安全信息#a。

其中，具体的判断逻辑和实现方式可参考上述方法 500 的步骤 S512 的相关描述，为了简洁，此处不再赘述。

S712，V-SMF 向 H-SMF 发送授权通知响应消息；对应的，HSMF 接收来自 V-SMF 的授权通知响应消息。

其中，该授权通知响应消息中包含 V-EASDF 的安全信息#a 和 V-EASDF 的地址。

S713，H-SMF 生成 ePCO#β。

其中，ePCO#β 包括 V-EASDF 的安全信息#b 和 V-EASDF 的地址。具体实现方式可参考上述方法 600 的步骤 S613 的相关描述，为了简洁，此处不再赘述。

S714，H-SMF 向 V-SMF 发送 PDU 会话建立响应；对应的，V-SMF 接收来自 H-SMF 的 PDU 会话建立响应。

示例性的，PDU 会话建立响应可以是 Nsmf_PDUSession_Creat Response。其中，PDU 会话建立响应包括 ePCO#β。

S715，V-SMF 向 AMF 发送 N1N2 消息传输；对应的，AMF 接收来自 V-SMF 的 N1N2 消息传输。

S716，AMF 向 UE 发送 PDU 会话建立响应#α；对应的，UE 接收来自 AMF 的 PDU 会话建立响应#α。

S717，PDU 会话建立后续过程。

S718，UE 使用 V-EASDF 的安全信息#b，向 V-EASDF 发送具有安全保护的 DNS 消息；对应的，V-EASDF 接收来自 UE 的具有安全保护的 DNS 消息。

其中，上述步骤 S714 至 S718 的具体实现方式，以及交互消息的具体名称，可参考上述方法 600 的步骤 S614 和 S618 的相关描述，为了简洁，此处不再过多赘述。

本申请所揭示的方法，在 HR-SBO PDU 会话建立过程中，V-SMF 根据来自 H-SMF 的 HR-SBO 授权指示，向 H-SMF 提供 V-EASDF 的安全信息#a，使得在需要开启 DNS over (D)TLS 时，H-SMF 能够向 UE 发送包含 V-EASDF 的安全信息#b 的 ePCO#β。基于该实现方式，能够保护 V-EASDF 与 UE 之间的安全连接，维护网络安全通信。

图 8 是本申请实施例提供的通信方法 800 的流程示例图。该方法在 HR-SBO PDU 会话建立过程中，H-SMF 在确定 HR-SBO 授权通过的情况下，向 V-SMF 发送 HR-SBO 授权指示，以使得后续 V-SMF 在确定需要请求 HR-SBO PDU 会话时，向 H-SMF 提供 V-EASDF 安全信息#a，进而使得 H-SMF 能够确定向 UE 发送 V-EASDF 的安全信息#b。基于来自归属地的会话管理功能网元的 HR-SBO 授权信息，以及在确定 UE 满足 HR-SBO 会话建立条件的情况下，才确定并获取安全信息#a，安全性更高。如图 8 所示，该方法包括如下多个步骤。

S801，UE 注册流程，AMF 从 UDM 获取 HR-SBO 允许指示。

S802，UE 向 AMF 发送 PDU 会话建立请求#1；对应的，AMF 接收来自 UE 的 PDU 会话建立请求#1。

S803，AMF 选择 V-SMF。

S804，AMF 向 V-SMF 发送创建会话管理上下文请求；对应的，V-SMF 接收来自 AMF 的创建会话管理上下文请求。

S805，V-SMF 向 AMF 发送创建会话管理上下文响应；对应的，AMF 接收来自 V-SMF 的创建会话管理上下文响应。

S806，V-SMF 向 H-SMF 发送 PDU 会话建立请求#2；对应的，H-SMF 接收来自 V-SMF 的 PDU 会话建立请求#2。

S807，H-SMF 向 UDM 请求获取 SDM 信息；对应的，UDM 接收来自 H-SMF 的获取 SDM 信息的请

求。

S808，UDM 向 H-SMF 发送 SDM 信息；对应的，H-SMF 接收来自 UDM 的 SDM 信息。

其中，上述步骤 S801 至 S808 的具体实现方式，以及交互消息的具体名称或含义，可参考上述方法 600 的步骤 S601 至 S608 的相关描述，为了简洁，此处不再过多赘述。

S809，H-SMF 确定 HR-SBO 授权。

示例性的，H-SMF 根据来自 UDM 的 SDM 信息中的 HR-SBO 授权指示或 HR-SBO 授权信息，确定 HR-SBO 授权。

S810，H-SMF 向 V-SMF 发送 PDU 会话建立响应#2；对应的，V-SMF 接收来自 H-SMF 的 PDU 会话建立响应#2。

其中，PDU 会话建立响应#2 包括 HR-SBO 授权指示或 HR-SBO 授权信息。进一步地，V-SMF 本地存储 HR-SBO 授权指示或 HR-SBO 授权信息，用于后续在 V-SMF 确定请求需要 HR-SBO PDU 会话时向 H-SMF 提供 V-EASDF 安全信息#a。

可选地，若 H-SMF 在步骤 S806 接收到的 ePCO#1 中包含 DNS 服务器安全信息指示，和/或 DNS 服务器安全协议支持，则 PDU 会话建立响应#2 还可以包含 DNS 服务器安全信息指示，和/或 DNS 服务器安全协议支持。进一步地，V-SMF 可以本地存储 DNS 服务器安全信息指示，和/或 DNS 服务器安全协议支持。

可选地，PDU 会话建立响应#2 还可以包含 H-DNS 服务器的地址，和/或 H-DNS 服务器的安全信息，用于解析特定应用（如由 HPLMN 能够路由的）的地址。

可选地，PDU 会话建立响应#2 还可以包括 PDU 会话的用户面安全策略。进一步地，V-SMF 可以本地存储 PDU 会话的用户面安全策略。

S811，V-SMF 向 AMF 发送 N1N2 消息传输#1；对应的，AMF 接收来自 V-SMF 的 N1N2 消息传输#1。

S812，AMF 向 UE 发送 PDU 会话建立响应#1；对应的，UE 接收来自 AMF 的 PDU 会话建立响应#1。

S813，PDU 会话建立后续过程。

其中，步骤 S811 至 S813 的具体实现方式可参考上述方法 600 的步骤 S615 至 S617 的相关描述，为了简洁，此处不再赘述。

S814，V-SMF 判断 HR-SBO PDU 会话建立是否满足条件。

示例性的，V-SMF 根据来自 AMF 的 UE 的位置信息，确定当前 UE 已经移动到 EHE（即 V-EASDF）的服务范围，而且 V-SMF 在步骤 S810 之后本地存储有 HR-SBO 授权指示，因此 V-SM 可以确定 HR-SBO PDU 会话建立满足条件，随即可以获取并向 H-SMF 提供 V-EASDF 的安全信息#a。

S815，V-SMF 获取 V-EASDF 的安全信息#a。

其中，获取 V-EASDF 的安全信息#a 的具体实现方式，以及 V-EASDF 的安全信息#a 包含的具体内容可参考上述方法 400 的步骤 S406 的相关描述，为了简洁，此处不再赘述。

S816，V-SMF 向 H-SMF 发送 PDU 会话更新请求；对应的，H-SMF 接收来自 V-SMF 的 PDU 会话更新请求。

S817，H-SMF 生成 ePCO#2。

S818，H-SMF 向 V-SMF 发送 PDU 会话更新响应；对应的，V-SMF 接收来自 H-SMF 的 PDU 会话更新响应。

其中，上述步骤 S816 至 S818 的具体实现方式，以及交互消息的名称或含义，可参考上述方法 600 的步骤 S612 至 S614 的相关描述，为了简洁，此处不再赘述。

S819，V-SMF 向 AMF 发送 N1N2 消息传输；对应的，AMF 接收来自 V-SMF 的 N1N2 消息传输。

其中，N1N2 消息传输可以是 N1N2_MessageTransfer，该消息包含 N1 SM 容器，N1 SM 容器包括 ePCO#2，ePCO#2 包括 V-EASDF 的安全信息#b 和 V-EASDF 的地址。

S820，AMF 向 UE 发送 N1 SM 容器；对应的，UE 接收来自 AMF 的 N1 SM 容器。

S821，PDU 会话修改后续过程。

其中，PDU 会话修改的具体实现方式可参考 3GPP TS23.502 中的相关描述，为了简洁，此处不再赘述。

S822，UE 使用 V-EASDF 的安全信息#b，向 V-EASDF 发送具有安全保护的 DNS 消息；对应的，V-EASDF 接收来自 UE 的具有安全保护的 DNS 消息。

应理解，该 DNS 消息是被保护的，可以保证 UE 与 V-EASDF 之间的安全通信。

本申请所揭示的方法，基于 H-SMF 发送的 HR-SBO 授权指示或 HR-SBO 授权信息，V-SMF 可以在确定 HR-SBO PDU 会话建立满足条件时，向 H-SMF 提供 V-EASDF 的安全信息#a，使得需要开启 DNS over (D)TLS 时，H-SMF 能够向 UE 发送包含 V-EASDF 的安全信息#b 的 ePCO#2。基于该实现方式，能够保护 V-EASDF 与 UE 之间的安全连接，维护网络安全通信。

需要说明的是，本申请提供的技术方案同样适用于其他漫游场景，例如未来独立的非公共网络（stand-alone non-public network，SNPN）的架构支持的漫游场景。区别在于，需要将上述图 1 示出的 PLMN 中的 V-SMF 和 H-SMF 分别替换成 SNPN 中不同私网中的 SMF。

上文结合图 1 至图 8，详细描述了本申请的通信方法侧实施例，下面将结合图 9 和图 10，详细描述本申请的终端设备侧实施例。应理解，装置实施例的描述与方法实施例的描述相互对应，因此，未详细描述的部分可以参见前面方法实施例。

图 9 是本申请实施例提供的一种终端设备 1000 的示意性框图。如图 9 所示，该设备 1000 可以包括收发单元 1010 和处理单元 1020。收发单元 1010 可以与外部进行通信，处理单元 1020 用于进行数据处理。收发单元 1010 还可以称为通信接口或收发单元。

在一种可能的设计中，该设备 1000 可实现对应于上文方法实施例中的通信装置（例如 UE）执行的步骤或者流程，其中，处理单元 1020 用于执行上文方法实施例中 UE 的处理相关的操作，收发单元 1010 用于执行上文方法实施例中 UE 的收发相关的操作。

在另一种可能的设计中，该设备 1000 可实现对应于上文方法实施例中的拜访地的会话管理功能网元（例如 V-SMF）执行的步骤或者流程，其中，收发单元 1010 用于执行上文方法实施例中 V-SMF 的收发相关的操作，处理单元 1020 用于执行上文方法实施例中 V-SMF 的处理相关的操作。

在又一种可能的设计中，该设备 1000 可实现对应于上文方法实施例中的归属地的会话管理功能网元（例如 H-SMF）执行的步骤或者流程，其中，收发单元 1010 用于执行上文方法实施例中 H-SMF 的收发相关的操作，处理单元 1020 用于执行上文方法实施例中 H-SMF 的处理相关的操作。

应理解，这里的设备 1000 以功能单元的形式体现。这里的术语“单元”可以指应用特有集成电路（application specific integrated circuit，ASIC）、电子电路、用于执行一个或多个软件或固件程序的处理器（例如共享处理器、专有处理器或组处理器等）和存储器、合并逻辑电路和/或其它支持所描述的功能的合适组件。在一个可选例子中，本领域技术人员可以理解，设备 1000 可以具体为上述实施例中的发送端，可以用于执行上述方法实施例中与发送端对应的各个流程和/或步骤，或者，设备 1000 可以具体为上述实施例中的接收端，可以用于执行上述方法实施例中与接收端对应的各个流程和/或步骤，为避免重复，在此不再赘述。

上述各个方案的设备 1000 具有实现上述方法中发送端所执行的相应步骤的功能，或者，上述各个方案的设备 1000 具有实现上述方法中接收端所执行的相应步骤的功能。所述功能可以通过硬件实现，也可以通过硬件执行相应的软件实现。所述硬件或软件包括一个或多个与上述功能相对应的模块；例如收发单元可以由收发机替代（例如，收发单元中的发送单元可以由发送机替代，收发单元中的接收单元可以由接收机替代），其它单元，如处理单元等可以由处理器替代，分别执行各个方法实施例中的收发操作以及相关的处理操作。

此外，上述收发单元还可以是收发电路（例如可以包括接收电路和发送电路），处理单元可以是处理电路。在本申请的实施例，图 9 中的装置可以是前述实施例中的接收端或发送端，也可以是芯片或者芯片系统，例如：片上系统（system on chip，SoC）。其中，收发单元可以是输入输出电路、通信接口。处理单元为该芯片上集成的处理器或者微处理器或者集成电路。在此不做限定。

图 10 是本申请实施例提供的另一种终端设备 2000 的示意性框图。如图 10 所示，该设备 2000 包括处理器 2010 和收发器 2020。其中，处理器 2010 和收发器 2020 通过内部连接通路互相通信，该处理器 2010 用于执行指令，以控制该收发器 2020 发送信号和/或接收信号。

可选地，该设备 2000 还可以包括存储器 2030，该存储器 2030 与处理器 2010、收发器 2020 通过内部连接通路互相通信。该存储器 2030 用于存储指令，该处理器 2010 可以执行该存储器 2030 中存储的指令。

在一种可能的实现方式中，设备 2000 用于实现上述方法实施例中的通信装置（例如 UE）对应的各个流程和步骤。

在另一种可能的实现方式中，设备 2000 用于实现上述方法实施例中的拜访地的会话管理功能网元

（例如 V-SMF）对应的各个流程和步骤。

在又一种可能的实现方式中，设备 2000 用于实现上述方法实施例中的归属地的会话管理功能网元（例如 H-SMF）对应的各个流程和步骤。

应理解，设备 2000 可以具体为上述实施例中的发送端或接收端，也可以是芯片或者芯片系统。对应的，该收发器 2020 可以是该芯片的收发电路，在此不做限定。具体地，该设备 2000 可以用于执行上述方法实施例中与发送端或接收端对应的各个步骤和/或流程。

可选地，该存储器 2030 可以包括只读存储器和随机存取存储器，并向处理器提供指令和数据。存储器的一部分还可以包括非易失性随机存取存储器。例如，存储器还可以存储设备类型的信息。该处理器 2010 可以用于执行存储器中存储的指令，并且当该处理器 2010 执行存储器中存储的指令时，该处理器 2010 用于执行上述与发送端或接收端对应的方法实施例的各个步骤和/或流程。

在实现过程中，上述方法的各步骤可以通过处理器中的硬件的集成逻辑电路或者软件形式的指令完成。结合本申请实施例所公开的方法的步骤可以直接体现为硬件处理器执行完成，或者用处理器中的硬件及软件模块组合执行完成。软件模块可以位于随机存储器，闪存、只读存储器，可编程只读存储器或者电可擦写可编程存储器、寄存器等本领域成熟的存储介质中。该存储介质位于存储器，处理器读取存储器中的信息，结合其硬件完成上述方法的步骤。为避免重复，这里不再详细描述。

应注意，本申请实施例中的处理器可以是一种集成电路芯片，具有信号的处理能力。在实现过程中，上述方法实施例的各步骤可以通过处理器中的硬件的集成逻辑电路或者软件形式的指令完成。上述的处理器可以是通用处理器、数字信号处理器、专用集成电路、现场可编程门阵列或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件。本申请实施例中的处理器可以实现或者执行本申请实施例中的公开的各方法、步骤及逻辑框图。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。结合本申请实施例所公开的方法的步骤可以直接体现为硬件译码处理器执行完成，或者用译码处理器中的硬件及软件模块组合执行完成。软件模块可以位于随机存储器，闪存、只读存储器，可编程只读存储器或者电可擦写可编程存储器、寄存器等本领域成熟的存储介质中。该存储介质位于存储器，处理器读取存储器中的信息，结合其硬件完成上述方法的步骤。

可以理解，本申请实施例中的存储器可以是易失性存储器或非易失性存储器，或可包括易失性和非易失性存储器两者。其中，非易失性存储器可以是只读存储器（read-only memory，ROM）、可编程只读存储器（programmable ROM，PROM）、可擦除可编程只读存储器（erasable PROM，EPROM）、电可擦除可编程只读存储器（electrically EPROM，EEPROM）或闪存。易失性存储器可以是随机存取存储器（random access memory，RAM），其用作外部高速缓存。通过示例性但不是限制性说明，许多形式的 RAM 可用，例如静态随机存取存储器、动态随机存取存储器、同步动态随机存取存储器、双倍数据速率同步动态随机存取存储器、增强型同步动态随机存取存储器、同步连接动态随机存取存储器和直接内存总线随机存取存储器。应注意，本文描述的系统和方法的存储器旨在包括但不限于这些和任意其它适合类型的存储器。

图 11 是本申请实施例提供的一种芯片系统 3000 的示意图。该芯片系统 3000（或者也可以称为处理系统）包括逻辑电路 3010 以及输入/输出接口（input/output interface）3020。

其中，逻辑电路 3010 可以为芯片系统 3000 中的处理电路。逻辑电路 3010 可以耦合连接存储单元，调用存储单元中的指令，使得芯片系统 3000 可以实现本申请各实施例的方法和功能。输入/输出接口 3020，可以为芯片系统 3000 中的输入输出电路，将芯片系统 3000 处理好的信息输出，或将待处理的数据或信令信息输入芯片系统 3000 进行处理。

作为一种方案，该芯片系统 3000 用于实现上文各个方法实施例中由通信装置（如图 2 至图 8 中的 UE）执行的操作。例如，逻辑电路 3010 用于实现上文方法实施例中由 UE 执行的处理相关的操作；输入/输出接口 3020 用于实现上文方法实施例中由 UE 执行的发送和/或接收相关的操作。

作为另一种方案，该芯片系统 3000 用于实现上文各个方法实施例中由拜访地的会话管理功能网元（如图 2 至图 8 中的 V-SMF）执行的操作。例如，逻辑电路 3010 用于实现上文方法实施例中由 V-SMF 执行的处理相关的操作；输入/输出接口 3020 用于实现上文方法实施例中由 V-SMF 执行的发送和/或接收相关的操作。

作为又一种方案，该芯片系统 3000 用于实现上文各个方法实施例中由拜访地的会话管理功能网元（如图 2 至图 8 中的 H-SMF）执行的操作。例如，逻辑电路 3010 用于实现上文方法实施例中由 H-SMF

执行的处理相关的操作；输入/输出接口 3020 用于实现上文方法实施例中由 H-SMF 执行的发送和/或接收相关的操作。

本申请实施例还提供一种计算机可读存储介质，其上存储有用于实现上述各方法实施例中由设备（例如 UE，或者 V-SMF，或者 H-SMF）执行的方法的计算机指令。

本申请实施例还提供一种计算机程序产品，包含指令，该指令被计算机执行时以实现上述各方法实施例中由设备（例如 UE，或者 V-SMF，或者 H-SMF）执行的方法。

本申请实施例还提供一种通信的系统，包括前述的例如 UE，或者 V-SMF，或者 H-SMF 中的一个或多个。

上述提供的任一种装置中相关内容的解释及有益效果均可参考上文提供的对应的方法实施例，此处不再赘述。

本领域普通技术人员可以意识到，结合本文中所公开的实施例描述的各示例的单元及算法步骤，能够以电子硬件、或者计算机软件和电子硬件的结合来实现。这些功能究竟以硬件还是软件方式来执行，取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能，但是这种实现不应认为超出本申请的范围。

所属领域的技术人员可以清楚地了解到，为描述的方便和简洁，上述描述的系统、装置和单元的具体工作过程，可以参考前述方法实施例中的对应过程，在此不再赘述。

在本申请所提供的几个实施例中，应该理解到，所揭露的系统、装置和方法，可以通过其它的方式实现。例如，以上所描述的装置实施例仅是示意性的，例如，所述单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，例如多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另一点，所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口，装置或单元的间接耦合或通信连接，可以是电性，机械或其它的形式。

所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

另外，在本申请各个实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。

所述功能如果以软件功能单元的形式实现并作为独立的产品销售或使用时，可以存储在一个计算机可读取存储介质中。基于这样的理解，本申请的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备等）执行本申请各个实施例所述方法的全部或部分步骤。而前述的存储介质包括：U 盘、移动硬盘、只读存储器、随机存取存储器、磁碟或者光盘等各种可以存储程序代码的介质。

以上所述，仅为本申请的具体实施方式，但本申请的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本申请揭露的技术范围内，可轻易想到变化或替换，都应涵盖在本申请的保护范围之内。因此，本申请的保护范围应以所述权利要求的保护范围为准。

# 权 利 要 求 书

1. 一种通信方法，其特征在于，所述方法应用于建立或修改终端设备的会话过程中，包括：

拜访地的会话管理功能网元获取位于所述拜访地的域名系统 DNS 服务器的安全信息和所述 DNS 服务器的标识，所述安全信息用于所述终端设备与所述 DNS 服务器之间建立安全连接；

所述拜访地的会话管理功能网元向归属地的会话管理功能网元发送所述安全信息和所述 DNS 服务器的标识；

所述拜访地的会话管理功能网元接收来自所述归属地的会话管理功能网元的协议配置选项 PCO，所述 PCO 包括所述安全信息和所述 DNS 服务器的标识；

所述拜访地的会话管理功能网元将所述 PCO 发送给所述终端设备。

2. 根据权利要求 1 所述的方法，其特征在于，所述安全信息包括用于认证所述 DNS 服务器的凭证。

3. 根据权利要求 2 所述的方法，其特征在于，所述安全信息还包括所述 DNS 服务器支持的一种或者多种安全协议类型，和/或建立所述安全连接所使用的端口号。

4. 根据权利要求 2 所述的方法，其特征在于，在所述拜访地的会话管理功能网元接收来自所述归属地的会话管理功能网元的 PCO 之前，所述方法还包括：

所述拜访地的会话管理功能网元向所述归属地的会话管理功能网元发送所述 DNS 服务器支持的一种或者多种安全协议类型，和/或建立所述安全连接所使用的端口号；

其中，所述 PCO 中还包括所述 DNS 服务器支持的一种或者多种安全协议类型中的一个或者多个安全协议类型和/或所述端口号。

5. 根据权利要求 1 至 4 中任一项所述的方法，其特征在于，来自所述归属地的会话管理功能网元的所述 PCO 为第一 PCO；在所述拜访地的会话管理功能网元获取位于所述拜访地的 DNS 服务器的安全信息之前，所述方法还包括：

所述拜访地的会话管理功能网元接收来自所述终端设备的第二 PCO，其中，所述第二 PCO 包括用于指示所述终端设备支持基于安全协议对 DNS 消息进行安全保护的指示信息；

所述拜访地的会话管理功能网元向所述归属地的会话管理功能网元发送所述第二 PCO；

所述拜访地的会话管理功能网元接收来自所述归属地的会话管理功能网元的请求消息，所述请求消息包括所述指示信息；

其中，所述拜访地的会话管理功能网元获取位于所述拜访地的 DNS 服务器的安全信息，包括：

响应于所述指示信息，所述拜访地的会话管理功能网元获取所述安全信息。

6. 根据权利要求 1 至 4 中任一项所述的方法，其特征在于，在所述拜访地的会话管理功能网元获取位于所述拜访地的 DNS 服务器的安全信息和所述 DNS 服务器的标识之前，所述方法还包括：

所述拜访地的会话管理功能网元接收来自移动和接入管理功能网元的归属地路由会话疏导 HR-SBO 允许指示；

其中，所述拜访地的会话管理功能网元获取位于所述拜访地的 DNS 服务器的安全信息和所述 DNS 服务器的标识，包括：

所述拜访地的会话管理功能网元根据所述 HR-SBO 允许指示，获取所述安全信息和所述 DNS 服务器的标识。

7. 根据权利要求 1 至 4 中任一项所述的方法，其特征在于，在所述拜访地的会话管理功能网元获取位于所述拜访地的 DNS 服务器的安全信息之前，所述方法还包括：

所述拜访地的会话管理功能网元接收来自所述归属地的会话管理功能网元的所述归属地的网络标识；

其中，所述拜访地的会话管理功能网元获取位于所述拜访地的 DNS 服务器的安全信息，包括：

所述拜访地的会话管理功能网元根据所述终端设备的所述网络标识，获取所述安全信息。

8. 根据权利要求 1 至 7 中任一项所述的方法，其特征在于，所述方法还包括：

所述拜访地的会话管理功能网元获取策略信息，所述策略信息用于指示所述归属地的会话管理功能网元向所述终端设备发送所述安全信息的触发条件；

所述拜访地的会话管理功能网元向所述归属地的会话管理功能网元发送所述策略信息。

9. 根据权利要求 1 至 4 中任一项所述的方法，其特征在于，在所述拜访地的会话管理功能网元获取位于所述拜访地的 DNS 服务器的安全信息之前，所述方法还包括：

所述拜访地的会话管理功能网元接收来自所述归属地的会话管理功能网元的与所述会话对应的用户面安全策略；其中，所述用户面安全策略指示不开启或者可选开启用户面安全保护；

其中，所述拜访地的会话管理功能网元获取位于所述拜访地的DNS服务器的安全信息，包括：

所述拜访地的会话管理功能网元根据所述用户面安全策略，获取所述安全信息。

10．根据权利要求1至4中任一项所述的方法，其特征在于，在所述拜访地的会话管理功能网元获取位于所述拜访地的DNS服务器的安全信息和所述DNS服务器的标识之前，所述方法还包括：

所述拜访地的会话管理功能网元接收来自所述归属地的会话管理功能网元的HR-SBO授权信息；

其中，所述拜访地的会话管理功能网元获取位于所述拜访地的DNS服务器的安全信息和所述DNS服务器的标识，包括：

所述拜访地的会话管理功能网元根据所述HR-SBO授权信息，获取所述安全信息和所述DNS服务器的标识。

11．根据权利要求10所述的方法，其特征在于，所述拜访地的会话管理功能网元根据所述HR-SBO授权信息，获取所述安全信息和所述DNS服务器的标识，包括：

在确定所述终端设备满足HR-SBO会话建立条件的情况下，所述拜访地的会话管理功能网元根据所述HR-SBO授权信息，获取所述安全信息和所述DNS服务器的标识。

12．根据权利要求1至11中任一项所述的方法，其特征在于，所述DNS服务器为边缘服务器发现功能网元。

13．根据权利要求1至12中任一项所述的方法，其特征在于，所述方法还包括：

所述拜访地的会话管理功能网元接收来自网络功能存储库功能网元的所述安全信息。

14．一种通信方法，其特征在于，所述方法应用于建立或修改终端设备的会话过程中，包括：

归属地的会话管理功能网元接收来自拜访地的会话管理功能网元的域名系统DNS服务器的安全信息和所述DNS服务器的标识，所述安全信息用于所述终端设备与所述DNS服务器之间建立安全连接；

所述归属地的会话管理功能网元生成协议配置选项PCO，所述PCO包括所述安全信息和所述DNS服务器的标识；

所述归属地的会话管理功能网元通过所述拜访地的会话管理功能网元向所述终端设备发送所述PCO。

15．根据权利要求14所述的方法，其特征在于，所述安全信息包括用于认证所述DNS服务器的凭证。

16．根据权利要求15所述的方法，其特征在于，所述安全信息还包括所述DNS服务器支持的一种或者多种安全协议类型，和/或建立所述安全连接所使用的端口号。

17．根据权利要求15所述的方法，其特征在于，在所述归属地的会话管理功能网元向所述拜访地的会话管理功能网元发送所述PCO之前，所述方法还包括：

所述归属地的会话管理功能网元接收来自所述拜访地的会话管理功能网元的所述DNS服务器支持的一种或者多种安全协议类型，和/或建立所述安全连接所使用的端口号；

其中，所述PCO中还包括所述DNS服务器支持的一种或者多种安全协议类型中的一个或者多个安全协议类型和/或所述端口号。

18．根据权利要求14至17中任一项所述的方法，其特征在于，所述方法还包括：

所述归属地的会话管理功能网元向统一数据管理功能网元发送签约数据管理请求消息；

所述归属地的会话管理功能网元接收来自所述统一数据管理功能网元的签约数据管理响应消息，其中，所述签约数据管理响应消息包括归属地路由会话疏导HR-SBO授权信息；

其中，所述归属地的会话管理功能网元生成PCO，包括：

响应于所述HR-SBO授权信息，所述归属地的会话管理功能网元生成所述PCO。

19．根据权利要求14至18中任一项所述的方法，其特征在于，在所述归属地的会话管理功能网元接收来自拜访地的会话管理功能网元的DNS服务器的安全信息之前，所述方法还包括：

所述归属地的会话管理功能网元向所述拜访地的会话管理功能网元发送所述HR-SBO授权信息，所述HR-SBO授权信息用于请求获取所述安全信息和所述DNS服务器的标识。

20．根据权利要求14至18中任一项所述的方法，其特征在于，所述归属地的会话管理功能网元生成的PCO为第一PCO；在所述归属地的会话管理功能网元生成PCO之前，所述方法还包括：

所述归属地的会话管理功能网元接收来自所述拜访地的会话管理功能网元的第二PCO，所述第二

PCO包括用于指示所述终端设备支持基于安全协议对DNS消息进行安全保护的指示信息；

所述归属地的会话管理功能网元向所述拜访地的会话管理功能网元发送请求消息，所述请求消息包括所述指示信息。

21. 根据权利要求20所述的方法，其特征在于，所述第二PCO还包括所述终端设备支持的一种或者多种安全协议类型；

其中，所述归属地的会话管理功能网元生成PCO，包括：

所述归属地的会话管理功能网元根据所述终端设备支持的一种或者多种安全协议类型，以及所述DNS服务器支持的一种或者多种安全协议类型，生成所述第一PCO，其中，所述第一PCO还包括所述DNS服务器与所述终端设备都支持的一个或者多个安全协议类型。

22. 根据权利要求14至18中任一项所述的方法，其特征在于，在所述归属地的会话管理功能网元生成PCO之前，所述方法还包括：

所述归属地的会话管理功能网元向所述拜访地的会话管理功能网元发送用户面安全策略，其中，所述用户面安全策略用于指示不开启或者可选开启用户面安全保护。

23. 根据权利要求14至18中任一项所述的方法，其特征在于，在所述归属地的会话管理功能网元生成PCO之前，所述方法还包括：

所述归属地的会话管理功能网元向所述拜访地的会话管理功能网元发送所述归属地的网络标识。

24. 根据权利要求14至22中任一项所述的方法，其特征在于，所述归属地的会话管理功能网元生成PCO，包括：

所述归属地的会话管理功能网元接收来自所述拜访地的会话管理功能网元的策略信息；其中，所述策略信息用于指示所述归属地的会话管理功能网元向所述终端设备发送所述安全信息的触发条件；

在满足所述触发条件的情况下，所述归属地的会话管理功能网元生成所述PCO。

25. 根据权利要求14至24中任一项所述的方法，其特征在于，所述DNS服务器为边缘服务器发现功能网元。

26. 一种通信方法，其特征在于，所述方法应用于建立或修改终端设备的会话过程中，包括：

通信装置通过拜访地的会话管理功能网元向归属地的会话管理功能网元发送第二协议配置选项PCO，所述第二PCO包括用于指示所述通信装置支持基于安全协议对DNS消息进行安全保护的指示信息；

所述通信装置通过所述拜访地的会话管理功能网元接收来自所述归属地的会话管理功能网元的第一PCO，其中，所述第一PCO包括所安全信息和位于所述拜访地的域名系统DNS服务器的标识；

所述通信装置基于所述安全信息，建立与所述DNS服务器之间安全连接。

27. 根据权利要求26所述的方法，其特征在于，所述安全信息包括用于认证所述DNS服务器的凭证。

28. 根据权利要求27所述的方法，其特征在于，所述安全信息还包括所述DNS服务器支持的一种或者多种安全协议类型，和/或建立所述安全连接所使用的端口号。

29. 根据权利要求26至28中任一项所述的方法，其特征在于，所述第二PCO还包括所述通信装置支持的一种或者多种安全协议类型；

其中，所述第一PCO还包括所述DNS服务器支持的一种或者多种安全协议类型中的一个或者多个安全协议类型。

30. 根据权利要求24至27中任一项所述的方法，其特征在于，所述DNS服务器为边缘服务器发现功能网元。

31. 一种通信方法，其特征在于，所述方法应用于建立或修改终端设备的会话过程中，包括：

拜访地的会话管理功能网元获取位于所述拜访地的域名系统DNS服务器的安全信息和所述DNS服务器的标识，所述安全信息用于所述终端设备与所述DNS服务器之间建立安全连接；

所述拜访地的会话管理功能网元向归属地的会话管理功能网元发送所述安全信息和所述DNS服务器的标识，所述归属地的会话管理功能网元接收来自所述拜访地的会话管理功能网元的所述安全信息和所述DNS服务器的标识；

所述归属地的会话管理功能网元生成协议配置选项PCO，所述PCO包括所述安全信息和所述DNS服务器的标识；

所述归属地的会话管理功能网元向所述拜访地的会话管理功能网元发送所述PCO，所述拜访地的会

话管理功能网元接收来自所述归属地的会话管理功能网元的PCO；

所述拜访地的会话管理功能网元将所述 PCO 发送给所述终端设备，所述终端设备接收来自所述拜访地的会话管理功能网元的所述PCO。

32．根据权利要求31所述的方法，其特征在于，所述方法还包括：

所述通信装置基于所述安全信息，建立与所述DNS服务器之间安全连接。

33．根据权利要求 31 或 32 所述的方法，其特征在于，所述安全信息包括用于认证所述 DNS 服务器的凭证。

34．根据权利要求 33 所述的方法，其特征在于，所述安全信息还包括所述 DNS 服务器支持的一种或者多种安全协议类型，和/或建立所述安全连接所使用的端口号。

35．根据权利要求 31 至 34 中任一项所述的方法，其特征在于，在所述归属地的会话管理功能网元向所述拜访地的会话管理功能网元发送所述PCO之前，所述方法还包括：

所述拜访地的会话管理功能网元向所述归属地的会话管理功能网元发送所述 DNS 服务器支持的一种或者多种安全协议类型，和/或建立所述安全连接所使用的端口号，所述归属地的会话管理功能网元接收来自所述拜访地的会话管理功能网元的所述 DNS 服务器支持的一种或者多种安全协议类型，和/或建立所述安全连接所使用的端口号；

其中，所述 PCO 中还包括所述 DNS 服务器支持的一种或者多种安全协议类型中的一个或者多个安全协议类型和/或所述端口号。

36．根据权利要求 31 至 35 中任一项所述的方法，其特征在于，所述归属地的会话管理功能网元生成的 PCO 为第一 PCO；在所述拜访地的会话管理功能网元获取位于所述拜访地的 DNS 服务器的安全信息之前，所述方法还包括：

所述终端设备向所述拜访地的会话管理功能网元发送第二 PCO，所述拜访地的会话管理功能网元接收来自所述终端设备的第二 PCO，其中，所述第二 PCO 包括用于指示所述终端设备支持基于安全协议对DNS 消息进行安全保护的指示信息；

所述拜访地的会话管理功能网元向所述归属地的会话管理功能网元发送所述第二 PCO，所述归属地的会话管理功能网元接收来自所述拜访地的会话管理功能网元的所述第二PCO；

所述归属地的会话管理功能网元向所述拜访地的会话管理功能网元发送请求消息，所述拜访地的会话管理功能网元接收来自所述归属地的会话管理功能网元的请求消息，所述请求消息包括所述指示信息；

其中，所述拜访地的会话管理功能网元获取位于所述拜访地的DNS服务器的安全信息，包括：

响应于所述指示信息，所述拜访地的会话管理功能网元获取所述安全信息。

37．根据权利要求36所述的方法，其特征在于，所述第二PCO还包括所述终端设备支持的一种或者多种安全协议类型；

其中，所述归属地的会话管理功能网元生成PCO，包括：

所述归属地的会话管理功能网元根据所述终端设备支持的一种或者多种安全协议类型，以及所述 DNS 服务器支持的一种或者多种安全协议类型，生成所述第一 PCO，其中，所述第一 PCO 还包括所述DNS服务器与所述终端设备都支持的一个或者多个安全协议类型。

38．根据权利要求 31 至 35 中任一项所述的方法，其特征在于，在所述拜访地的会话管理功能网元获取位于所述拜访地的DNS服务器的安全信息和所述DNS服务器的标识之前，所述方法还包括：

移动和接入管理功能网元向所述拜访地的会话管理功能网元发送归属地路由会话疏导 HR-SBO 允许指示，所述拜访地的会话管理功能网元接收来自所述移动和接入管理功能网元的归属地路由会话疏导HR-SBO允许指示；

其中，所述拜访地的会话管理功能网元获取位于所述拜访地的 DNS 服务器的安全信息和所述 DNS服务器的标识，包括：

所述拜访地的会话管理功能网元根据所述 HR-SBO 允许指示，获取所述安全信息和所述 DNS服务器的标识。

39．根据权利要求31至35中任一项所述的方法，其特征在于，所述方法还包括：

所述归属地的会话管理功能网元向统一数据管理功能网元发送签约数据管理请求消息，所述统一数据管理功能网元接收来自所述归属地的会话管理功能网元的所述签约数据管理请求消息；

所述统一数据管理功能网元向所述归属地的会话管理功能网元发送签约数据管理响应消息，所述归

属地的会话管理功能网元接收来自所述统一数据管理功能网元的所述签约数据管理响应消息，其中，所述签约数据管理响应消息包括 HR-SBO 授权信息；

其中，所述归属地的会话管理功能网元生成 PCO，包括：

响应于所述 HR-SBO 授权信息，所述归属地的会话管理功能网元生成所述 PCO。

40．根据权利要求 39 所述的方法，其特征在于，在所述归属地的会话管理功能网元接收来自拜访地的会话管理功能网元的 DNS 服务器的安全信息之前，所述方法还包括：

所述归属地的会话管理功能网元向所述拜访地的会话管理功能网元发送所述 HR-SBO 授权信息，所述拜访地的会话管理功能网元接收来自所述归属地的会话管理功能网元的所述 HR-SBO 授权信息，所述 HR-SBO 授权信息用于请求获取所述安全信息和所述 DNS 服务器的标识；

其中，所述拜访地的会话管理功能网元获取位于所述拜访地的 DNS 服务器的安全信息和所述 DNS 服务器的标识，包括：

所述拜访地的会话管理功能网元根据所述 HR-SBO 授权信息，获取所述安全信息和所述 DNS 服务器的标识。

41．根据权利要求 40 所述的方法，其特征在于，所述拜访地的会话管理功能网元根据所述 HR-SBO 授权信息，获取所述安全信息和所述 DNS 服务器的标识，包括：

在确定所述终端设备满足 HR-SBO 会话建立条件的情况下，所述拜访地的会话管理功能网元根据所述 HR-SBO 授权信息，获取所述安全信息和所述 DNS 服务器的标识。

42．根据权利要求 31 至 41 中任一项所述的方法，其特征在于，在所述拜访地的会话管理功能网元获取位于所述拜访地的 DNS 服务器的安全信息之前，所述方法还包括：

所述归属地的会话管理功能网元向所述拜访地的会话管理功能网元发送用户面安全策略，所述拜访地的会话管理功能网元接收来自所述归属地的会话管理功能网元的所述用户面安全策略，其中，所述用户面安全策略指示不开启或者可选开启用户面安全保护；

其中，所述拜访地的会话管理功能网元获取位于所述拜访地的 DNS 服务器的安全信息，包括：

所述拜访地的会话管理功能网元根据所述用户面安全策略，获取所述安全信息。

43．根据权利要求 31 至 41 中任一项所述的方法，其特征在于，在所述拜访地的会话管理功能网元获取位于所述拜访地的 DNS 服务器的安全信息之前，所述方法还包括：

所述归属地的会话管理功能网元向所述拜访地的会话管理功能网元发送所述归属地的网络标识，所述拜访地的会话管理功能网元接收来自所述归属地的会话管理功能网元的所述归属地的网络标识；

其中，所述拜访地的会话管理功能网元获取位于所述拜访地的 DNS 服务器的安全信息，包括：

所述拜访地的会话管理功能网元根据所述终端设备的所述网络标识，获取所述安全信息。

44．根据权利要求 31 至 43 中任一项所述的方法，其特征在于，所述归属地的会话管理功能网元生成 PCO，包括：

所述拜访地的会话管理功能网元获取策略信息，所述策略信息用于指示所述归属地的会话管理功能网元向所述终端设备发送所述安全信息的触发条件；

所述拜访地的会话管理功能网元向所述归属地的会话管理功能网元发送所述策略信息，所述归属地的会话管理功能网元接收来自所述拜访地的会话管理功能网元的所述策略信息；

在满足所述触发条件的情况下，所述归属地的会话管理功能网元生成所述 PCO。

45．根据权利要求 31 至 44 中任一项所述的方法，其特征在于，所述 DNS 服务器为边缘服务器发现功能网元。

46．一种通信系统，其特征在于，包括：拜访地的会话管理功能网元和归属地的会话管理功能网元，其中，所述拜访地的会话管理功能网元用于执行如权利要求 1 至 13 中任一项所述的方法，所述归属地的会话管理功能网元用于执行如权利要求 14 至 25 中任一项所述的方法。

47．根据权利要求 46 所述的通信系统，其特征在于，所述通信系统还包括终端设备，所述终端设备用于执行如权利要求 26 至 30 中任一项所述的方法。

48．一种通信装置，其特征在于，包括：一个或多个功能模块，所述一个或多个功能模块或网元用于执行如权利要求 1 至 13 中任一项所述的方法，或者，所述一个或多个功能模块或网元用于执行如权利要求 14 至 25 中任一项所述的方法，或者，所述一个或多个功能模块或网元用于执行如权利要求 26 至 30

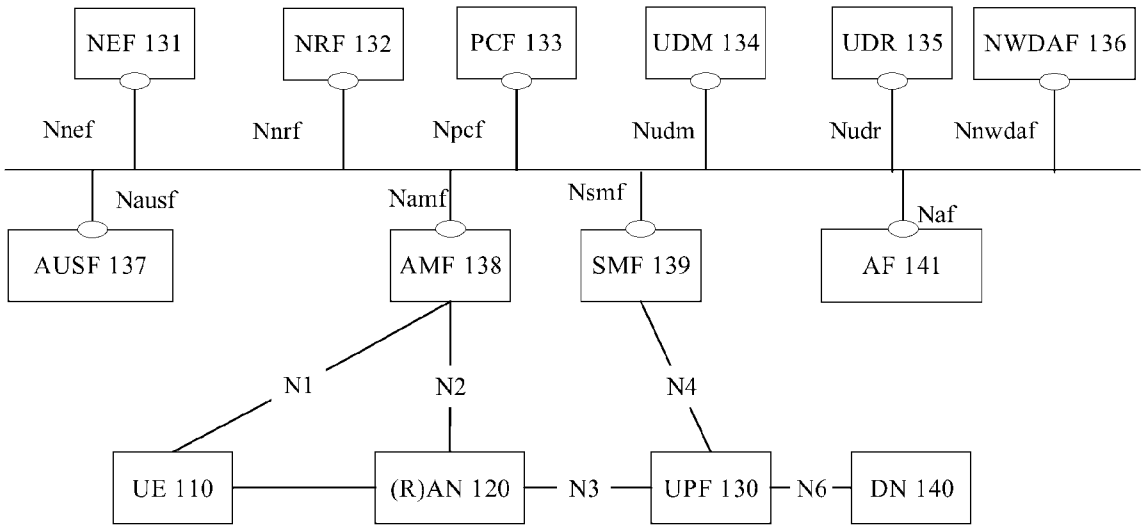
中任一项所述的方法。

49. 一种通信装置，其特征在于，包括：处理器，所述处理器与存储器耦合；所述处理器，用于执行所述存储器中存储的计算机程序，以使得所述装置执行如权利要求 1 至 13 中任一项所述的方法，或者以使得所述装置执行如权利要求 14 至 25 中任一项所述的方法，或者以使得所述装置执行如权利要求 26 至 30 中任一项所述的方法。

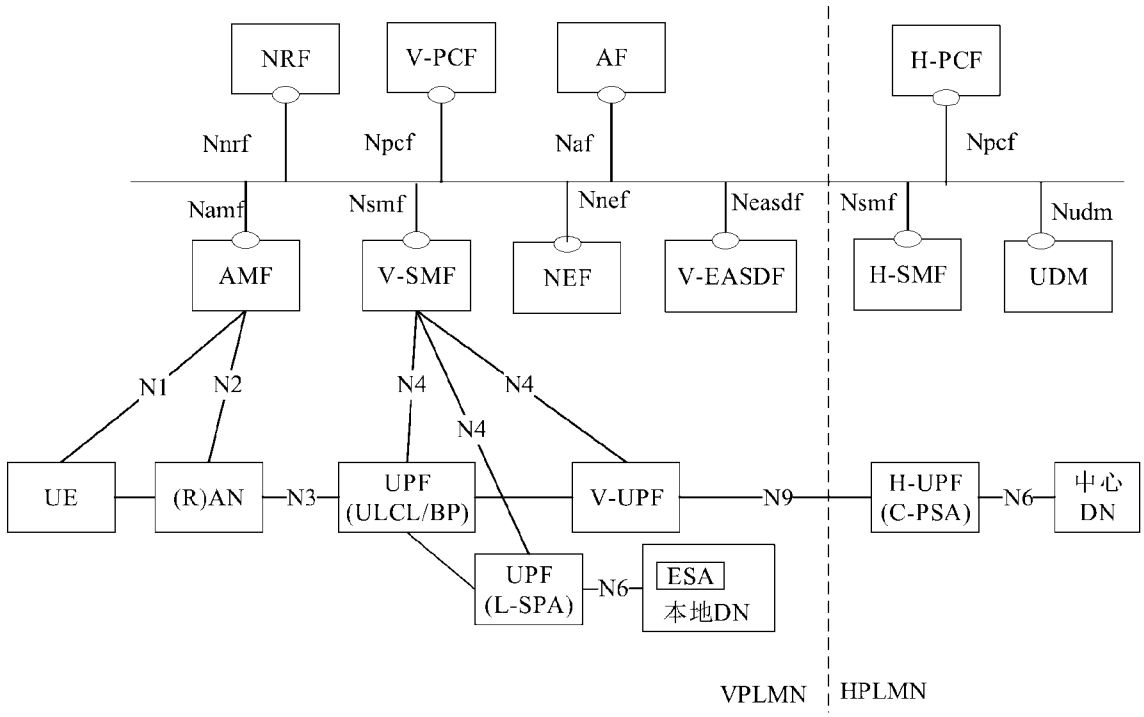
50. 一种计算机可读存储介质，其特征在于，包括：所述计算机可读存储介质上存储有计算机程序代码或指令，当所述计算机程序代码或指令运行时，使得所述计算机执行如权利要求 1 至 13 中任一项所述的方法，或者使得所述计算机执行如权利要求 14 至 25 中任一项所述的方法，或者使得所述计算机执行如权利要求 26 至 30 中任一项所述的方法。

51. 一种计算机程序产品，其特征在于，所述计算机程序产品被通信装置执行时，实现如权利要求 1 至 13 中任一项所述的方法，或者实现如权利要求 14 至 25 中任一项所述的方法，或者实现如权利要求 26 至 30 中任一项所述的方法。

52. 一种芯片，其特征在于，包括：处理器，用于从存储器中调用并运行计算机程序，使得安装有所述芯片的通信装置执行如权利要求 1 至 13 中任一项所述的方法，或者使得安装有所述芯片的通信装置执行如权利要求 14 至 25 中任一项所述的方法，或者使得安装有所述芯片的通信装置执行如权利要求 26 至 30 中任一项所述的方法。


NEF 131
NRF 132
PCF 133
UDM 134
UDR 135
NWDAF 136
Nnef
Nnrf
Npcf
Nudm
Nudr
Nnwdaf
Nausf
Namf
Nsmf
Naf
AUSF 137
AMF 138
SMF 139
AF 141
N1
N2
N4
UE 110
(R)AN 120
N3
UPF 130
N6
DN 140

(a)


NRF
V-PCF
AF
H-PCF
Nnrf
Npcf
Naf
Npcf
Namf
Nsmf
Nnef
Neasdf
Nsmf
Nudm
AMF
V-SMF
NEF
V-EASDF
H-SMF
UDM
N1
N2
N4
N4
N4
UE
(R)AN
N3
UPF
(ULCL/BP)
V-UPF
N9
H-UPF
(C-PSA)
N6
中心
DN
UPF
(L-SPA)
N6
ESA
本地DN
VPLMN
HPLMN

(b)

图 1

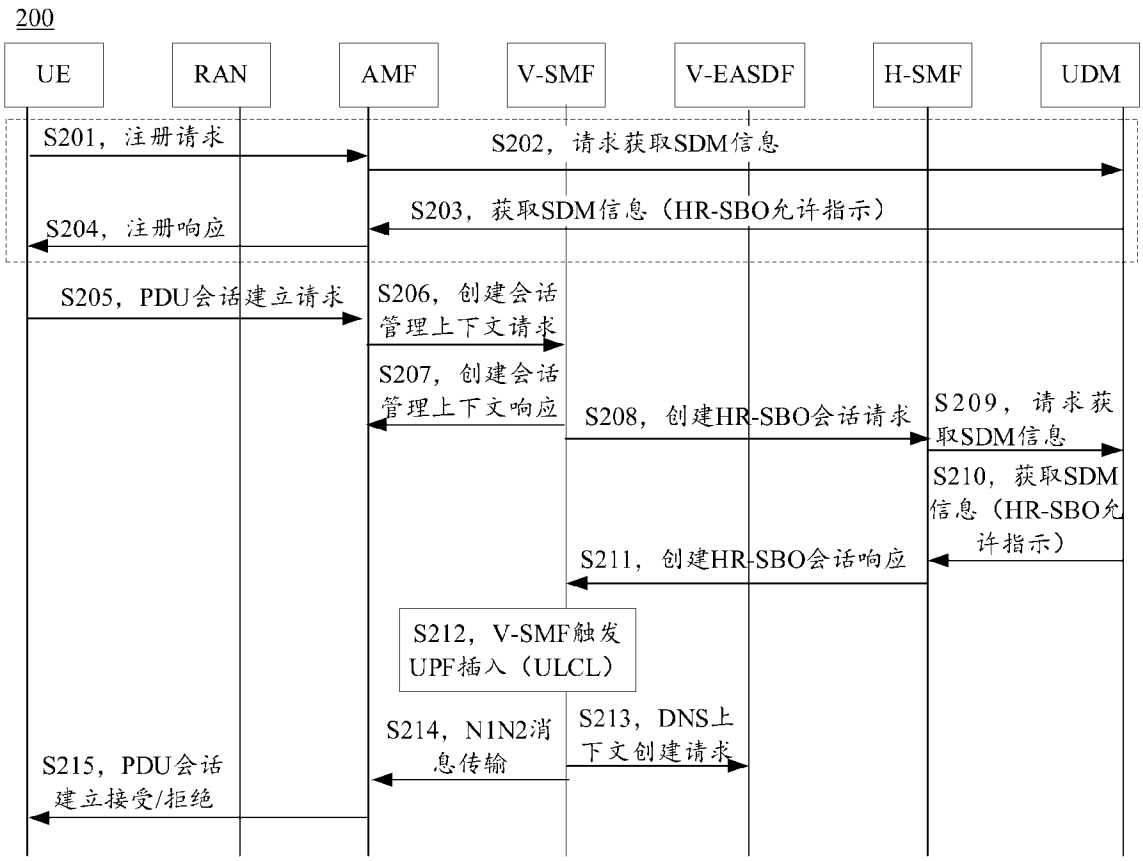

200
UE
RAN
AMF
V-SMF
V-EASDF
H-SMF
UDM
S201，注册请求
S202，请求获取SDM信息
S203，获取SDM信息（HR-SBO允许指示）
S204，注册响应
S205，PDU会话建立请求
S206，创建会话管理上下文请求
S207，创建会话管理上下文响应
S208，创建HR-SBO会话请求
S209，请求获取SDM信息
S210，获取SDM信息（HR-SBO允许指示）
S211，创建HR-SBO会话响应
S212，V-SMF触发UPF插入（ULCL）
S213，DNS上下文创建请求
S214，N1N2消息传输
S215，PDU会话建立接受/拒绝

图 2

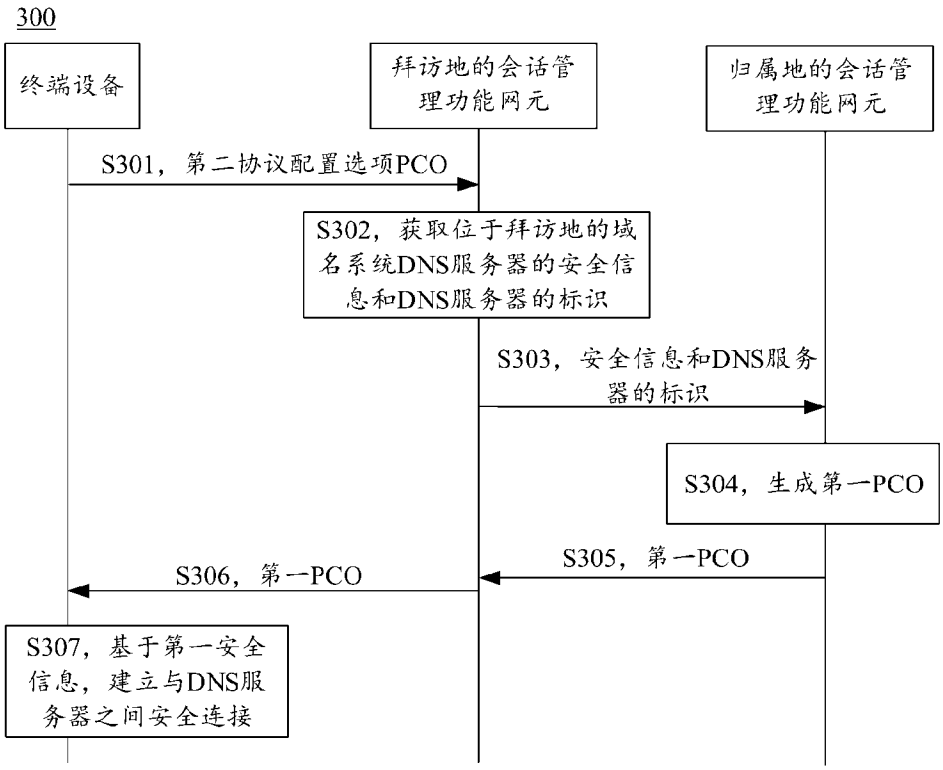

300
终端设备
拜访地的会话管理功能网元
归属地的会话管理功能网元
S301，第二协议配置选项PCO
S302，获取位于拜访地的域名系统DNS服务器的安全信息和DNS服务器的标识
S303，安全信息和DNS服务器的标识
S304，生成第一PCO
S305，第一PCO
S306，第一PCO
S307，基于第一安全信息，建立与DNS服务器之间安全连接

图 3

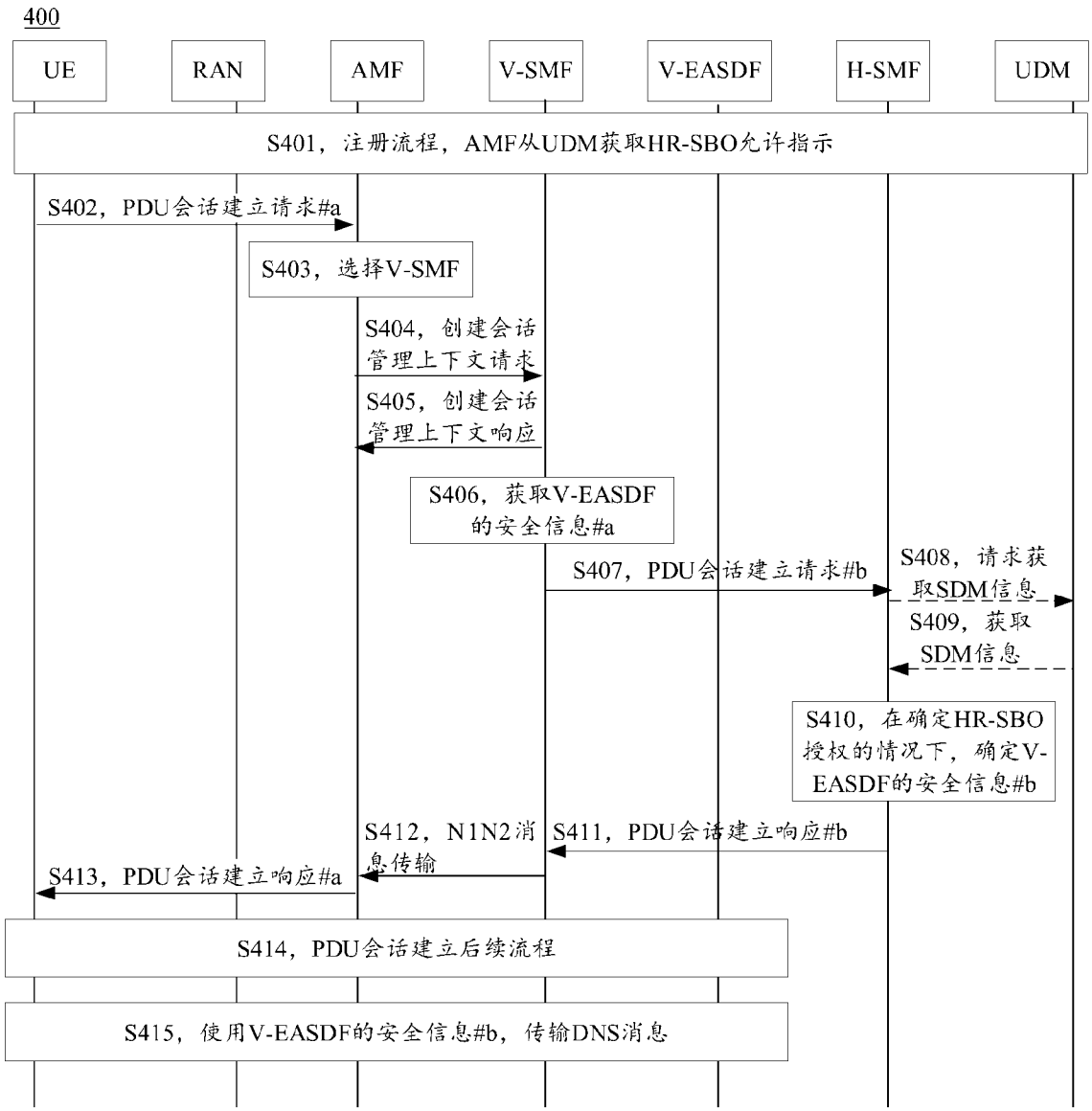

400
UE
RAN
AMF
V-SMF
V-EASDF
H-SMF
UDM
S401，注册流程，AMF从UDM获取HR-SBO允许指示
S402，PDU会话建立请求#a
S403，选择V-SMF
S404，创建会话管理上下文请求
S405，创建会话管理上下文响应
S406，获取V-EASDF的安全信息#a
S407，PDU会话建立请求#b
S408，请求获取SDM信息
S409，获取SDM信息
S410，在确定HR-SBO授权的情况下，确定V-EASDF的安全信息#b
S411，PDU会话建立响应#b
S412，N1N2消息传输
S413，PDU会话建立响应#a
S414，PDU会话建立后续流程
S415，使用V-EASDF的安全信息#b，传输DNS消息

图 4

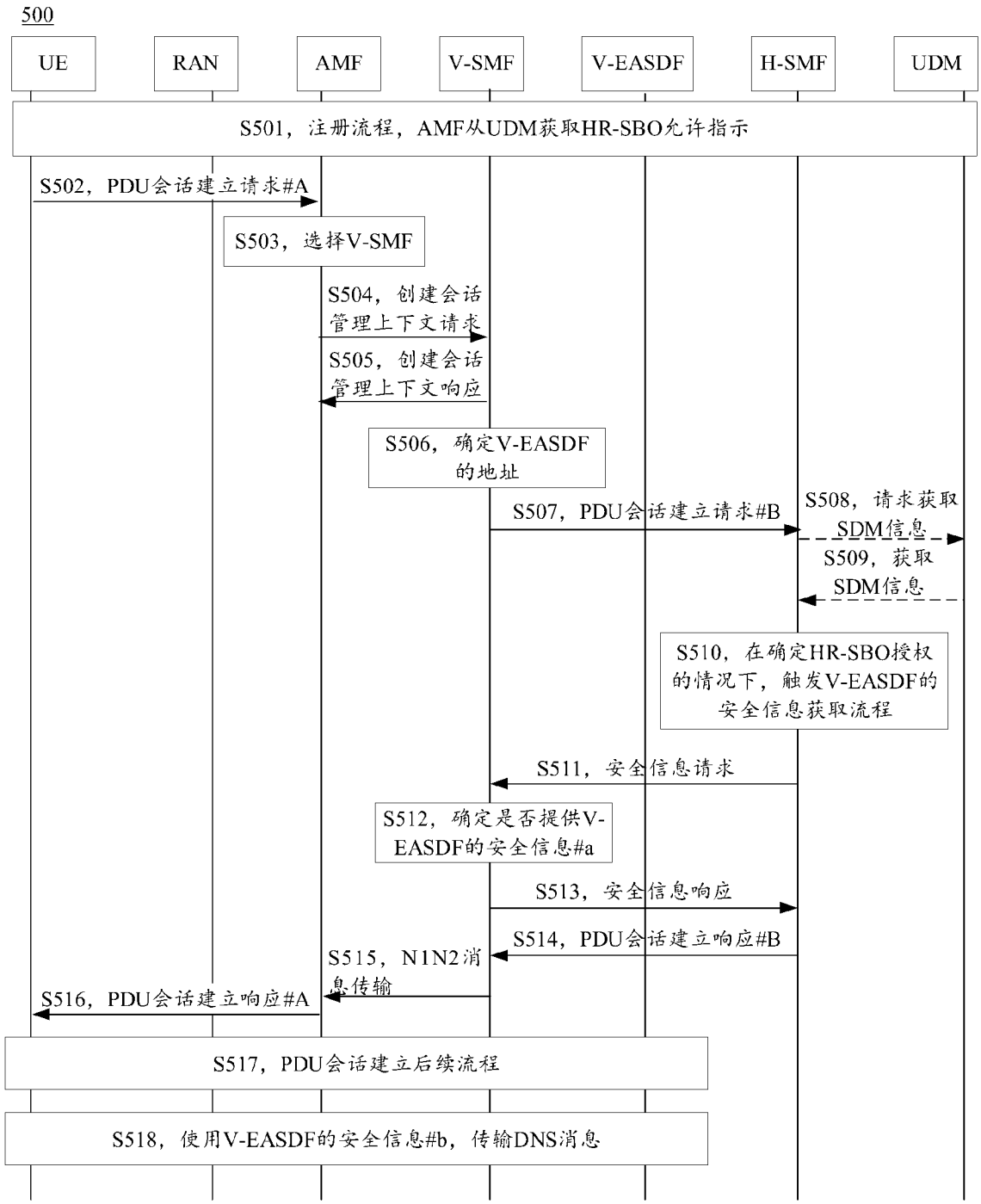

500
UE
RAN
AMF
V-SMF
V-EASDF
H-SMF
UDM
S501，注册流程，AMF从UDM获取HR-SBO允许指示
S502，PDU会话建立请求#A
S503，选择V-SMF
S504，创建会话管理上下文请求
S505，创建会话管理上下文响应
S506，确定V-EASDF的地址
S507，PDU会话建立请求#B
S508，请求获取SDM信息
S509，获取SDM信息
S510，在确定HR-SBO授权的情况下，触发V-EASDF的安全信息获取流程
S511，安全信息请求
S512，确定是否提供V-EASDF的安全信息#a
S513，安全信息响应
S514，PDU会话建立响应#B
S515，N1N2消息传输
S516，PDU会话建立响应#A
S517，PDU会话建立后续流程
S518，使用V-EASDF的安全信息#b，传输DNS消息

图 5

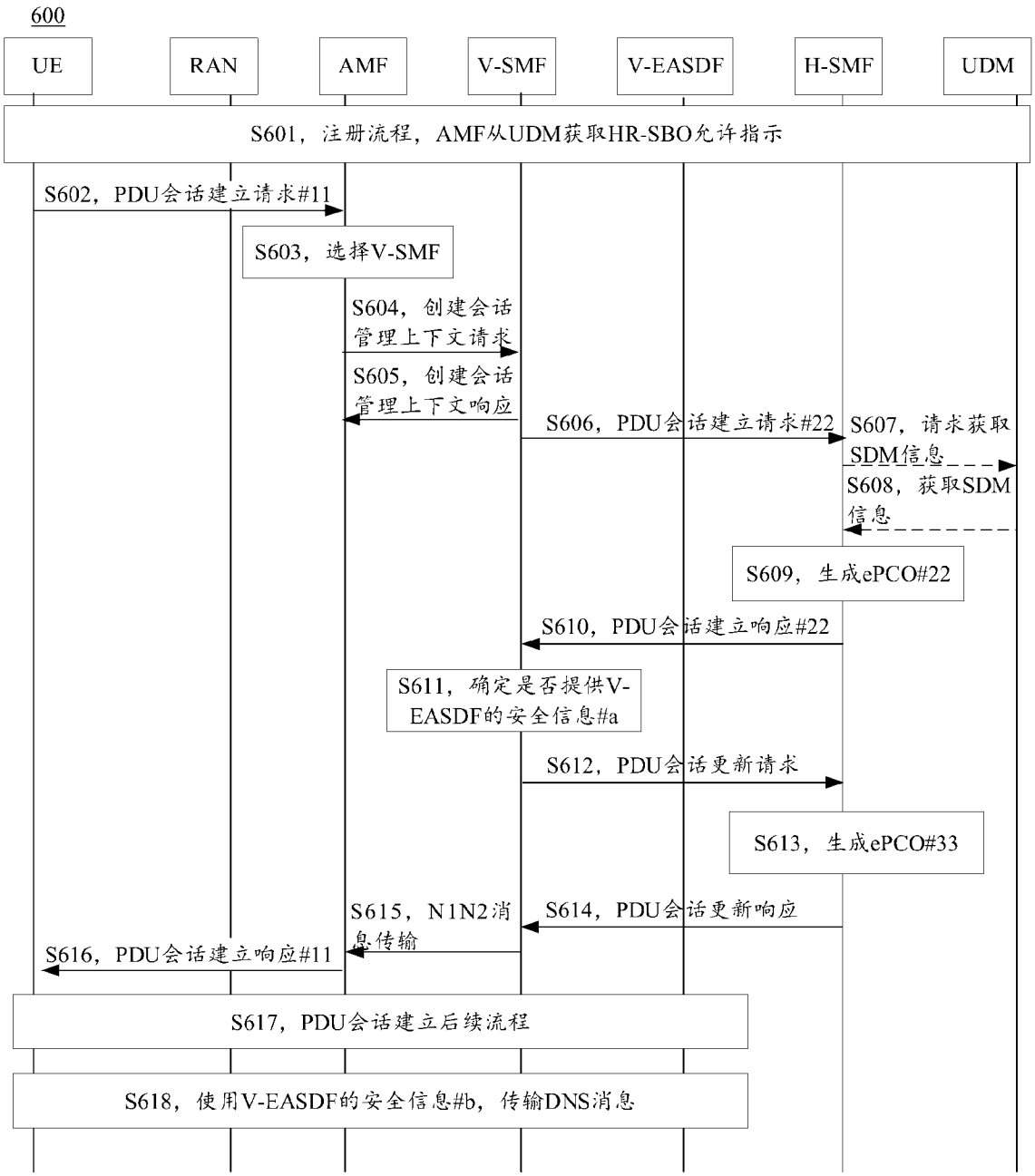

600
UE
RAN
AMF
V-SMF
V-EASDF
H-SMF
UDM
S601，注册流程，AMF从UDM获取HR-SBO允许指示
S602，PDU会话建立请求#11
S603，选择V-SMF
S604，创建会话管理上下文请求
S605，创建会话管理上下文响应
S606，PDU会话建立请求#22
S607，请求获取SDM信息
S608，获取SDM信息
S609，生成ePCO#22
S610，PDU会话建立响应#22
S611，确定是否提供V-EASDF的安全信息#a
S612，PDU会话更新请求
S613，生成ePCO#33
S614，PDU会话更新响应
S615，N1N2消息传输
S616，PDU会话建立响应#11
S617，PDU会话建立后续流程
S618，使用V-EASDF的安全信息#b，传输DNS消息

图 6

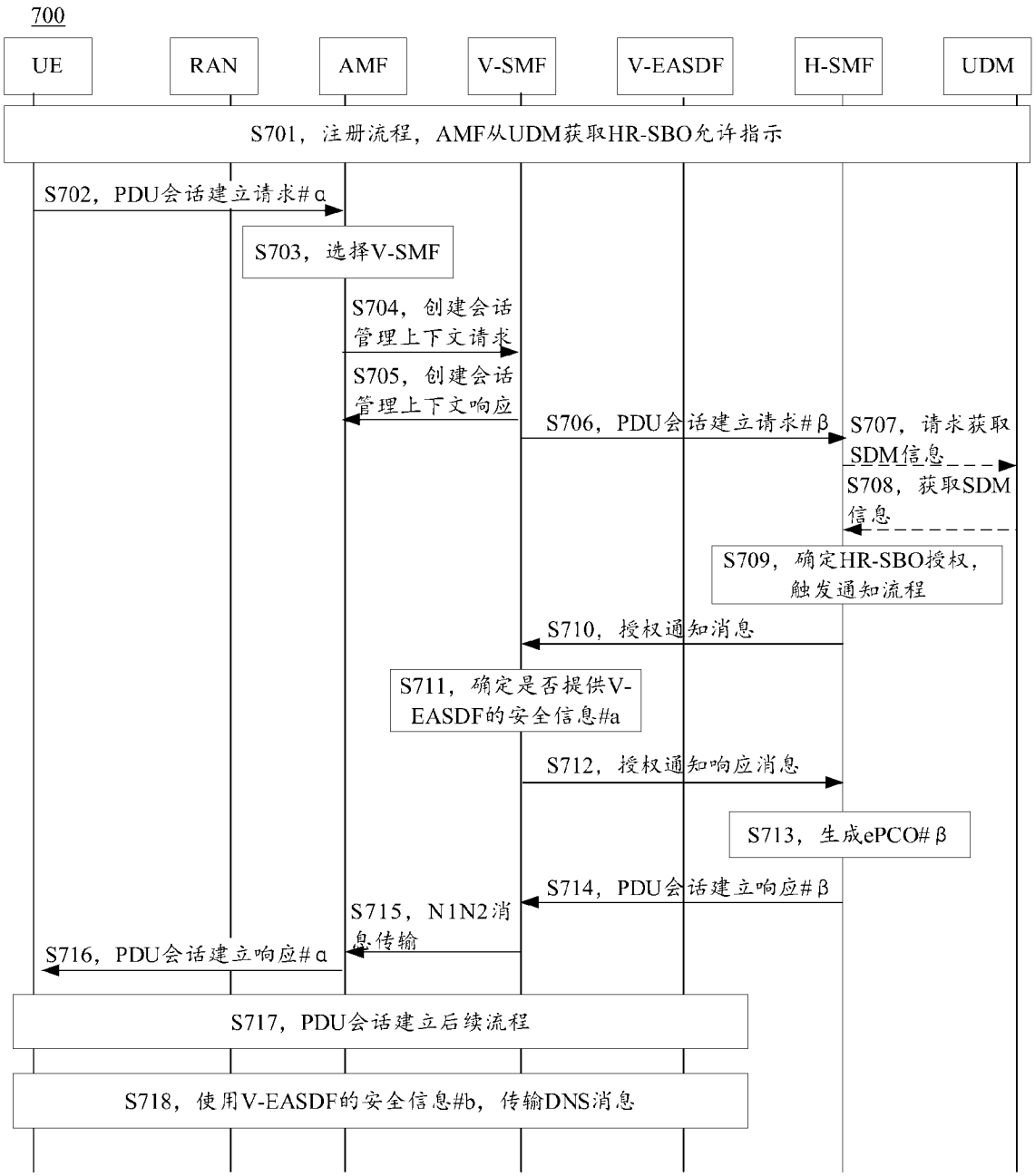

700
UE
RAN
AMF
V-SMF
V-EASDF
H-SMF
UDM
S701，注册流程，AMF从UDM获取HR-SBO允许指示
S702，PDU会话建立请求#α
S703，选择V-SMF
S704，创建会话管理上下文请求
S705，创建会话管理上下文响应
S706，PDU会话建立请求#β
S707，请求获取SDM信息
S708，获取SDM信息
S709，确定HR-SBO授权，触发通知流程
S710，授权通知消息
S711，确定是否提供V-EASDF的安全信息#a
S712，授权通知响应消息
S713，生成ePCO#β
S714，PDU会话建立响应#β
S715，N1N2消息传输
S716，PDU会话建立响应#α
S717，PDU会话建立后续流程
S718，使用V-EASDF的安全信息#b，传输DNS消息

图 7

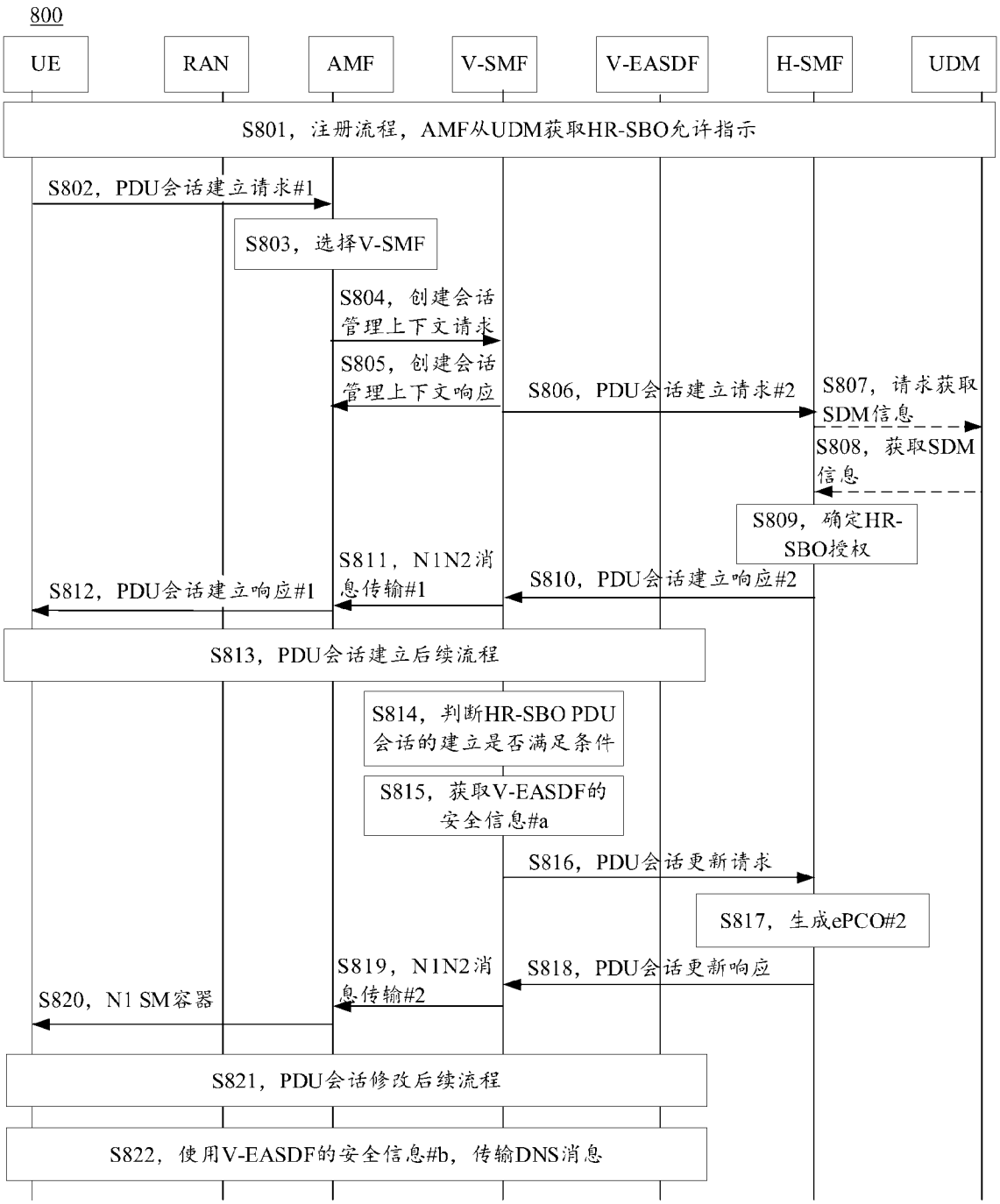

800
UE
RAN
AMF
V-SMF
V-EASDF
H-SMF
UDM
S801，注册流程，AMF从UDM获取HR-SBO允许指示
S802，PDU会话建立请求#1
S803，选择V-SMF
S804，创建会话管理上下文请求
S805，创建会话管理上下文响应
S806，PDU会话建立请求#2
S807，请求获取SDM信息
S808，获取SDM信息
S809，确定HR-SBO授权
S810，PDU会话建立响应#2
S811，N1N2消息传输#1
S812，PDU会话建立响应#1
S813，PDU会话建立后续流程
S814，判断HR-SBO PDU会话的建立是否满足条件
S815，获取V-EASDF的安全信息#a
S816，PDU会话更新请求
S817，生成ePCO#2
S818，PDU会话更新响应
S819，N1N2消息传输#2
S820，N1 SM容器
S821，PDU会话修改后续流程
S822，使用V-EASDF的安全信息#b，传输DNS消息

图 8

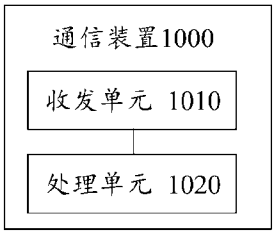

通信装置1000
收发单元 1010
处理单元 1020

图 9

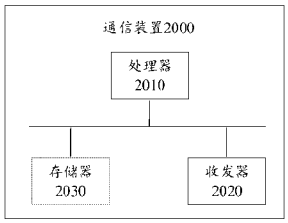

通信装置2000
处理器
2010
存储器
2030
收发器
2020

图 10

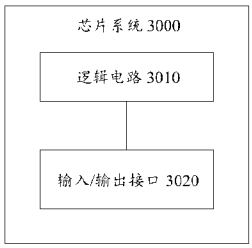

芯片系统 3000
逻辑电路 3010
输入/输出接口 3020

图 11

# INTERNATIONAL SEARCH REPORT

International application No.
**PCT/CN2024/070490**

## 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; CNTXT; CNKI; VEN; WOTXT; USTXT; EPTXT; 3GPP: 拜访地, 归属地, 会话管理网元, 边缘, 域名系统, 协议配置, 服务器, 发现功能网元, 安全, 接入, 标识, visited, SMF, home, edge, DNS, PCO, server, EASDF, safe, access, ID

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| Y | CN 114125808 A (CHINA UNITED NETWORK COMMUNICATIONS GROUP CO., LTD.) 01 March 2022 (2022-03-01)<br>description, paragraphs [0072]-[0143] | 1-52 |
| Y | CN 114286335 A (HUAWEI TECHNOLOGIES CO., LTD.) 05 April 2022 (2022-04-05)<br>description, paragraphs [0085]-[0119] | 1-52 |
| A | CN 112188574 A (HUAWEI TECHNOLOGIES CO., LTD.) 05 January 2021 (2021-01-05)<br>entire document | 1-52 |
| A | US 2020366794 A1 (SAMSUNG ELECTRONICS CO., LTD.) 19 November 2020 (2020-11-19)<br>entire document | 1-52 |

☐ 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 |
|---|---|
| **25 March 2024** | **05 April 2024** |

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

**INTERNATIONAL SEARCH REPORT**
**Information on patent family members**

International application No.
**PCT/CN2024/070490**

| Patent document cited in search report | Publication date (day/month/year) | Patent family member(s) | Publication date (day/month/year) |
|---|---|---|---|
| CN 114125808 A | 01 March 2022 | None | |
| CN 114286335 A | 05 April 2022 | None | |
| CN 112188574 A | 05 January 2021 | None | |
| US 2020366794 A1 | 19 November 2020 | US 11006004 B2 | 11 May 2021 |

# 国际检索报告

国际申请号
PCT/CN2024/070490

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;CNTXT;CNKI;VEN;WOTXT;USTXT;EPTXT;3GPP：拜访地，归属地，会话管理网元，边缘，域名系统，协议配置，服务器，发现功能网元，安全，接入，标识，visited，SMF，home，edge，DNS，PCO，server，EASDF，safe，access，ID

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 |
|---|---|---|
| Y | CN 114125808 A (中国联合网络通信集团有限公司) 2022年3月1日 (2022 - 03 - 01)<br>说明书第[0072]-[0143]段 | 1-52 |
| Y | CN 114286335 A (华为技术有限公司) 2022年4月5日 (2022 - 04 - 05)<br>说明书第[0085]-[0119]段 | 1-52 |
| A | CN 112188574 A (华为技术有限公司) 2021年1月5日 (2021 - 01 - 05)<br>全文 | 1-52 |
| A | US 2020366794 A1 (SAMSUNG ELECTRONICS CO LTD) 2020年11月19日 (2020 - 11 - 19)<br>全文 | 1-52 |

☐ 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3月25日 | 2024年4月5日 |
| ISA/CN的名称和邮寄地址<br>中国国家知识产权局<br>中国北京市海淀区蓟门桥西土城路6号 100088 | 受权官员<br>叶鼎晟<br>电话号码 (+86) 0512-88996125 |

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2024/070490

| 检索报告引用的专利文件 | 公布日<br>(年/月/日) | 同族专利 | 公布日<br>(年/月/日) |
|---|---|---|---|
| CN 114125808 A | 2022年3月1日 | 无 | |
| CN 114286335 A | 2022年4月5日 | 无 | |
| CN 112188574 A | 2021年1月5日 | 无 | |
| US 2020366794 A1 | 2020年11月19日 | US 11006004 B2 | 2021年5月11日 |