(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
11 August 2022 (11.08.2022)

WIPO | PCT

(10) International Publication Number
WO 2022/169693 A1

(51) International Patent Classification:
*H04W 8/08* (2009.01) *H04W 12/72* (2021.01)
*H04W 4/50* (2018.01) *H04W 84/10* (2009.01)
*H04W 12/069* (2021.01) *H04W 84/04* (2009.01)

(21) International Application Number:
PCT/US2022/014430

(22) International Filing Date:
28 January 2022 (28.01.2022)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
63/144,885 02 February 2021 (02.02.2021) US
63/151,006 18 February 2021 (18.02.2021) US

(71) Applicant: **INTEL CORPORATION** [US/US]; 2200 Mission College Boulevard, Santa Clara, California 95054 (US).

(72) Inventor: **LIAO, Ching-Yu**; 14557 NW Cosmos Street, Portland, Oregon 97229 (US).

(74) Agent: **MOORE, Michael S.** et al.; SCHWABE, WILLIAMSON & WYATT, P.C., 1211 SW 5th Avenue, Suite 1600, Portland, Oregon 97204 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

**Declarations under Rule 4.17:**
— *of inventorship (Rule 4.17(iv))*

**Published:**
— *with international search report (Art. 21(3))*

(54) Title: ROAMING BETWEEN PUBLIC AND NON-PUBLIC 5G NETWORKS

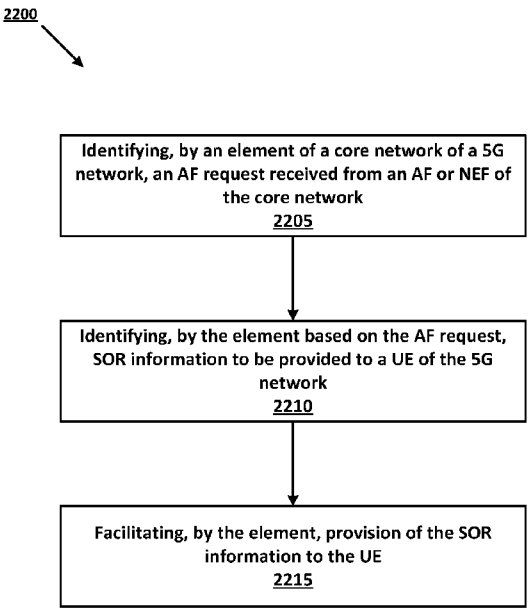


Figure 22

(57) Abstract: Various embodiments herein provide techniques related to roaming between public and non-public fifth generation (5G) networks. In one embodiment, techniques may be related to provisioning a user equipment (UE) with steering of roaming (SOR) information. In another embodiment, techniques may be related to providing access to a providing access to localized service (PALS) network through provisioning of the UE with one or more authentication parameters of the PALS network. Other embodiments may be described and/or claimed.

WO 2022/169693 A1

# ROAMING BETWEEN PUBLIC AND NON-PUBLIC 5G NETWORKS

## CROSS REFERENCE TO RELATED APPLICATION

The present application claims priority to U.S. Provisional Patent Application No. 63/144,885, which was filed February 2, 2021; U.S. Provisional Patent Application No. 63/151,006, which was filed February 18, 2021; and U.S. Provisional Patent Application No. 63/147,123, which was filed February 8, 2021.

## FIELD

Various embodiments generally may relate to the field of wireless communications. For example, some embodiments may relate to roaming between public and non-public fifth generation (5G) networks.

## BACKGROUND

Various embodiments generally may relate to the field of wireless communications.

## BRIEF DESCRIPTION OF THE DRAWINGS

Embodiments will be readily understood by the following detailed description in conjunction with the accompanying drawings. To facilitate this description, like reference numerals designate like structural elements. Embodiments are illustrated by way of example and not by way of limitation in the figures of the accompanying drawings.

Figure 1 depicts an example diagram for building relationship(s) between network operators using an application layer approach, in accordance with various embodiments.

Figure 2 depicts an example of an application function (AF) requesting to trigger one or more steering of roaming (SOR) updates to user equipments (UEs), in accordance with various embodiments.

Figure 3 depicts an example of Nnef_ParameterProvision_Create / Nnef_ParameterProvision_Update / Nnef_ParameterProvision_Delete request/response operations, in accordance with various embodiments.

Figure 4 depicts an example of service specific information provisioning, in accordance with various embodiments.

Figure 5 depicts an example of an overall non-roaming reference architecture of policy and charging control framework for the 5G System (service based representation), in accordance with various embodiments.

Figure 6 depicts an example of an overall non-roaming reference architecture of policy and charging control framework for the 5G System (reference point representation), in accordance with various embodiments.

Figure 7 schematically depicts an example of a SOR transparent container information

element for list type with value "0" and SOR data type with value "0," in accordance with various embodiments.

Figure 8 depicts an example of a SOR transparent container information element for list type with value "1" and SOR data type with value "0," in accordance with various embodiments.

Figure 9 depicts an example of a public land mobile network identifier (ID) and access technology list, in accordance with various embodiments.

Figure 10 depicts an example of a SOR transparent container information element for SOR data type with value "1," in accordance with various embodiments.

Figure 11 depicts an example of a SOR header for SOR data type with value “0,” in accordance with various embodiments.

Figure 12 depicts an example of a SOR header for SOR data type with value “1,” in accordance with various embodiments.

Figures 13A-B depict an example procedure for providing list of preferred PLMN/access technology combinations, in accordance with various embodiments.

Figure 14 depicts an example procedure for providing list of preferred PLMN/access technology combinations after registration, in accordance with various embodiments.

Figures 15A-B depict an example UE Configuration Update procedure for access and mobility management related parameters, in accordance with various embodiments.

Figure 16 depicts an example UE Configuration Update procedure for transparent UE Policy delivery, in accordance with various embodiments.

Figure 17 depicts an example diagram related to the relationship of security domains among network operators, in accordance with various embodiments.

Figure 18 depicts an example high level procedure for UE accessing home network services or on-demand services, in accordance with various embodiments.

Figure 19 depicts an example procedure for initiating hosting connectivity services for group users, in accordance with various embodiments.

Figure 20 depicts an example of a home operator owned/collaborative roaming scenario – home routed, in accordance with various embodiments.

Figure 21 depicts an example of a providing access to localized service (PALS) network operator owned/collaborative roaming scenario – local breakout, in accordance with various embodiments.

Figure 22 depicts an example technique related to roaming between public and non-public 5G networks, in accordance with various embodiments.

Figure 23 depicts an alternative example technique related to roaming between public and non-public 5G networks, in accordance with various embodiments.

Figure 24 schematically illustrates a wireless network in accordance with various embodiments.

Figure 25 schematically illustrates components of a wireless network in accordance with various embodiments.

Figure 26 is a block diagram illustrating components, according to some example embodiments, able to read instructions from a machine-readable or computer-readable medium (e.g., a non-transitory machine-readable storage medium) and perform any one or more of the methodologies discussed herein.

## DETAILED DESCRIPTION

The following detailed description refers to the accompanying drawings. The same reference numbers may be used in different drawings to identify the same or similar elements. In the following description, for purposes of explanation and not limitation, specific details are set forth such as particular structures, architectures, interfaces, techniques, etc. in order to provide a thorough understanding of the various aspects of various embodiments. However, it will be apparent to those skilled in the art having the benefit of the present disclosure that the various aspects of the various embodiments may be practiced in other examples that depart from these specific details. In certain instances, descriptions of well-known devices, circuits, and methods are omitted so as not to obscure the description of the various embodiments with unnecessary detail. For the purposes of the present document, the phrases "A or B" and "A/B" mean (A), (B), or (A and B).

Embodiments herein may relate to various mechanisms related to roaming between public and non-public 5G networks. Some mechanisms may relate to authentication and authorization for providing access to local services in 5G systems. Some mechanisms may relate to supporting collaborative roaming for providing access to local services in 5G systems. Some mechanisms may relate to steering user equipments (UEs) for roaming between public and non-public 5G systems. Other mechanisms may be described herein.

### Mechanisms for Steering UEs for Roaming Between Public and Non-Public 5G Networks

In third generation partnership project (3GPP), SP-200799 is a study item related to Providing Access to Localized Services (PALS). As used herein, a PALS network may refer to a hosting network that provides access to localized services as a PALS network. The use cases considered are, in certain places or areas, like a stadium, arena, airport, university campus, convention center etc., a 5G network (also known as a new radio (NR) network) may be deployed or available locally. The network may provide services for temporary events and access to services

on demand to local users. Such services may be offered by the 5G network operator, other mobile operator(s) or third party content provider(s), generating additional revenue opportunities. Some examples may include:

- Match video coverage and replay/statistics at a stadium (e.g. by sport content provider);
- High quality multimedia telephony (MMTEL)/streaming for on-campus or remote live events/concerts;
- Premium connectivity for real-time games or augmented reality/virtual reality (AR/VR) services at a gaming fair;
- On-demand services at a movie theater, commercial ads in shopping malls, etc.

The above use cases may need to enhance supports of a 5G network for UEs to access specific services offered by the service providers, including PLMN or NPN (non-public network) operator, or 3rd party service/content provider(s), via a 5G serving network in a on demand, temporary basis and/or at specific location(s). Figure 1 depicts an example diagram for building relationship(s) between network operators using an application layer approach, in accordance with various embodiments. Specifically, Figure 1 shows an example scenario related to accessing 5G PALS network (hosting network A).

An e-agreement may be established among service operators, e.g. SP-A, SP-B, and SP-C, that do not have a relevant or existing service-level agreements (SLAs) in place for the PALS services provided by SP-A's hosting network-A. Based on the PALS e-agreement, the hosting network may be configured with a PALS service at a specific time and location for its PALS service subscribers (other network operator), e.g. PALS service policies of time, location, network-A access parameters, including spectrum, access technologies (3GPP or non-3GPP), network slice, charging policies, and subscriber's network policies for authentication, and routing.

With the e-agreement, the trust relationship among service providers may be assumed. Embodiments herein provide example solutions to resolve the open issues in the following scenarios in Figure 1:

- Case 1: for steering UE from SP-C network to SP-A PALS network
  - The UE accessing to home network services via its home network (SP-C).
  - When the UE enters an area at a specific time, the SP-C steers the UE from SP-C network to SP-A's PALS network.
  - The UE can access PALS network to either continue its home network services or select on demand services via PALS network.
  - The steering of roaming is effective only for a specific time and location. After the occasion, the UE returns to its SP-C network or Equivalent home networks.
- Case 2: for UE continuing services from SP-C network to SP-A PALS network based on

the application requirements.

- The UE accessing to on demand services via its home network (SP-C).
- The user starts an application with premium option that requires better quality of service (QoS).
- The SP-C directs the UE to access SP-A's network providing the same on demand service when the UE is in the coverage of SP-A.

- There are other cases that may be considered by the SP-C to direct or steer the UEs to other PALS networks, e.g. performing load balancing to move UEs from one network to another network, (between home/visiting network/PALS network, between PALS networks).

Some open issues of the above use case include:

- Legacy SOR information update procedures for steering of UE in the visited PLMN (VPLMN) or home PLMN (HPLMN) by the network may only support the cases when the UE is trying to register onto the VPLMN or after the UE has registered onto the HPLMN. It not clear in the legacy specifications how to enhance the existing SOR update procedure or other procedures to support the above PALS network scenario which is in operation at a specific time and location and trigger criterion is based on location, time, application requirements or other causes.
- Legacy SOR information may only be applicable for steering of UEs among PLMN networks. Given that the PALS network may be a Standalone NPN (SNPN), it is not clear in the legacy specifications how to enhance the SoR information in SOR update procedure.

Embodiments herein may include or relate to the following service requirements and solutions:

-F: Example service requirements to enhance existing SOR update procedures for PALS.

-Solution 2: Example enhanced SOR update procedure with new trigger criterions and application inferences.

-Solution 3: Example SOR information enhancement for instructing the UE to select the HPLMN/home SNPN (HSNPN) preferred PALS network which may be a SNPN or PLMN.

**Solution 1: Example service requirements to enhance existing SOR update procedures for PALS**

1- The 5G system shall be able to allow home network provider directly or via visiting network to direct or steer UE(s) to a PALS network (SNPN or PLMN) based on the location, time, specific local services, or load balancing.

2- The 5G system shall be able to steer a UE to a PALS network (PLMN or NPN) for accessing to local services based on application request.

**Solution 2: Example enhancement for triggering SOR update procedure**

Embodiments of this solution may include enhancements to the legacy procedure in the 3GPP technical specification (TS) 23.122 for C.2 (Stage-2 flow for steering of UE in VPLMN during registration) and C.3 (Stage-2 flow for steering of UE in HPLMN or VPLMN after registration) for supporting a SNPN 5G network.

These procedures may be used as the control plane solution for steering of roaming in the 5G system (5GS).

Embodiments may include one or more of the following:

- Enhancement of the SOR update procedure such that the HPLMN/HSNPN provides protected list of preferred PLMN/access technology combinations via NAS signalling to the UE for updating the list of "Operator Controlled PLMN/SNPN Selector with Access Technology" in the UE.
- Enhancement of the triggering of SOR update procedure such that third party application can request for inferencing the SOR policy via AF/network exposure function (NEF). This enhancement may support the use case that an application needs to have better QoS which may be provided by different 5G network provider, e.g. PALS network for local services.

The enhanced procedure of embodiments herein may include one or more of the following aspects that differentiate it from the legacy procedures of C2 and C3 in 3GPP TS 23.122:

- The procedure may apply to updating SOR information containing network identities of PLMN and/or SNPN (standalone), e.g. PLMN ID for PLMN and PLMN-ID+NPN ID for SNPN.
- The procedure may apply to updating information of SOR via a downlink (DL) non-access stratum (NAS) message, UE configuration command or UE policy container to UEs after registration
- The procedure of updating SOR information may be triggered by an AF sending an AF request to Home network operator's unified data management (UDM) via NEF.
- The application function of an application server is different from AF-SOR for triggering SOR updates.

Figure 2 shows an example of the enhanced procedure for SOR update. Specifically, Figure 2 depicts an example of an AF requesting to trigger one or more SOR updates to user equipments (UEs), in accordance with various embodiments. Figure 2 may include or describe

one or more of the following:

Step1: AF to the HPLMN UDM via NEF:

AF request is sent to the HPLMN UDM via NEF to trigger the update of the UE with the new list of preferred PLMN/SNPN/access technology combinations or a secured packet for a UE.

The AF request message contains at least one of the following information:

- AF-Service-Identifier for indicating the AF request service
- Application IDs for SOR update
- External identifier for a UE or external Group Identifier for a group of UEs
- Desired Edge Data Network information, e.g. combination of data network name (DNN), single-network slice selection assistance information (S-NSSAI), and edge data network service provider (EDSP) for the applications
- SOR update indication
- SOR information including:
  - Network type, e.g. PALS network that provides access to PALS services (identified by the application ID).
  - Ordered lists of preferred PLMN/SNPN network identities.
  - SOR validity indication

Desired Edge Data Network information, e.g. combination of DNN, S-NSSAI, and EDSP (edge data network service provider) for the applications may indicate the supported EGSP for the list of the preferred PLMN/SNPN network. This information can be used during protocol data unit (PDU) session establishment procedure by the UE for a session management function (SMF) to select a proper EDSP.

The NEF authorizes the AF request received from the AF and stores the information in the unified data repository (UDR) as "Application Data". With SOR update indication from the AF request message, the UDR interacts with UDM for updating the SOR.

Step 2-9: these steps may be similar to those of the legacy 3GPP TS 23.122 clause C.3, stage-2 flow for steering of UE in HPLMN or VPLMN after registration with the following modification:

- Step3a/3b: between HPLMN/HSNPN and SOR-AF, the request message is Nsoraf_SOR update request which is to update roaming network information with the list of network identities provided by the AF to SOR-AF. In the Nsoraf_SOR update response message, the SOR-AF provides the list of preferred PLMN/SNPN/access technology combinations, or the secured packet, or neither of them. The list may be one integrated list which

contains both of PLMN ID and SNPN ID (PLMN ID + NPN ID) or two separated list including ordered list of PLMN ID/access technologies combinations or ordered list of SNPN ID/access technologies combinations.

Step 5 may be modified in accordance with one or more of the following Options (1, 2a, and/or 2b) as follows:

Option1: The DL NAS Transport message includes SOR transparent container.

The SOR transparent container may add a new information element (IE) of SOR validity indication which provides the location and the time to enforce the provided SOR information in the UE to perform network re-selection procedure based on updated SOR information.

- When the SOR validity indication is met and the UE is registered with Home/Visiting PLMN/SNPN network, the UE stores the old list of Operator Controlled PLMN/SNPN Selector with Access Technology" list and performs the network (re)-selection based on the ordered list of preferred PLMN/SNPN information provided in a SOR transparent container which SOR validity criteria is met.
- When the SOR validity indication of the updated SOR container becomes invalid, the UE restores the old list of Operator Controlled PLMN/SNPN Selector with Access Technology" list and applies for network (re)-selection or return back to the previous network based on the active application.

Option2a: The UE configuration command from access mobility function (AMF) includes SOR information.

The AMF uses UE configuration command to update the UE configuration with the information of: application identity information, SOR information containing associated ordered lists of preferred PLMN/SNPN network identities and SOR validity indications which provides the location and the time of the SOR configuration.

- Referenced procedure is referring to 3GPP TS 23.502 clause 4.2.4.2 with handling at the UE for managing “Operator Controlled PLMN/SNPN Selector with Access Technology" list based on the received UE configuration with information of application IDs, and associated SOR information including ordered lists of preferred PLMN/SNPN network identities, and SOR validity indications.

Option2b: The UE policy container is delivered by AMF transparently

The AMF received UE policy container from PCF and delivers the UE policy containing information of application identities information, SOR information containing associated ordered

lists of preferred PLMN/SNPN network identities and SOR validity indications which provides the location and the time of the SOR configuration.

- Referenced procedure is referring to TS23.502 clause 4.2.4.3 with handling at the UE for managing “Operator Controlled PLMN/SNPN Selector with Access Technology" list based on the received UE policy with information of application IDs and associated SOR information including ordered lists of preferred PLMN/SNPN network identities and SOR validity indications.

For option 2a and 2b:

- When the SOR validity indication is met for an application and the UE is registered with Home/Visiting PLMN/SNPN network and the UE is using the application, the UE stores the old list of Operator Controlled PLMN/SNPN Selector with Access Technology" list and performs the network (re)-selection based on the ordered list of preferred PLMN/SNPN information provided in a UE configuration.
- When the SOR validity indication becomes invalid or the UE stops using the associated application, the UE restores the old list of Operator Controlled PLMN/SNPN Selector with Access Technology" list and applies for network (re)-selection or return back to the previous network based on the active application.

Step10: The HPLMN UDM returns AF request response message when the procedure is completed. This step may be performed after step 2.

**Solution 2.1**

Following solution 2, the legacy procedure in 3GPP TS 23.502 clause 4.15.6.2 (shown as Figure 3 herein), NEF service operations information flow (to network function (NF), for UE and UE group), may be used to update SOR information and interact with HPLMN-UDM/UDR. Such a procedure is depicted in Figure 3. Specifically, Figure 3 depicts Figure 3 depicts an example of Nnef_ParameterProvision_Create / Nnef_ParameterProvision_Update / Nnef_ParameterProvision_Delete request/response operations, in accordance with various embodiments. The following may be noted:

- The AF request/response in solution 2, above, is the Nnef_ParameterProvision_Create / Nnef_ParameterProvision_Update / Nnef_ParameterProvision_Delete request/response operations.
- The NF in Figure 3 is the AMF which can trigger:
    - Option1: as indicated in solution 2 step 5 option1.
    - Option2: the UE configuration update procedures as indicated in solution 2

step 5 option 2.

**Solution 2.2**

Following solution 2, the legacy procedure in 3GPP TS 23.502 clause 4.15.6.7 (shown herein as Figure 4), Service specific information provisioning, may be used to update SOR information as specific parameters for a UE, a group of UE or any UE and interact with HPLMN-UDM/UDR. Specifically, Figure 4 depicts an example of service specific information provisioning, in accordance with various embodiments. This procedure may enable the AF to provide service specific parameters to 5G system via NEF and the AF may issue requests on behalf of applications not owned by the HPLMN/HSNPN serving the UE.

In this solution, UE policy is used for delivering SOR information associated to applications. Based on the SOR validity indication and active application, the UE determines to enforce the network (re)-selection as depicted in Solution2, step 5 option2a/2b.

- The AF request/response in solution 2 is the Nnef_ServiceParameter_Create / Nnef_ServiceParameter_Update /Nnef_ServiceParameter_Delete request/response operations.

**Solution2.3: redirecting UE to the target PLMN/SNPN network**

Following solution 2, this solution may use a new NAS message to allow the AMF directing the UE to the target PLMN/SNPN network requested by the AF.

The redirect target network command NAS message may be sent by the AMF which contains at least of one or more of the following redirection information:

- Redirection validity indications:
    - Application IDs
    - Validity time
    - Validity location
- Preferred network type indicating as PLMN or SNPN or both
- The ordered list of target network IDs which may be one merged list or two separated list including ordered list of preferred PLMN list and ordered list of preferred SNPN list.

For example, for the immediate redirection to a specific SNPN-1 case, the UE may automatically select an indicated SNPN-1 if the SNPN-1 is fulfilled the required signal qualities, in which the redirect target network command NAS message includes:

- Redirection validity indication: N/A
- Preferred network type: SNPN

- Ordered list of target network ID: SNPN-ID 1

For example, for the immediate redirection to an ordered list of preferred SNPNs case, the UE may present to the users for manual selection of SNPNs or performs automatic SNPN selections for the user, in which the redirect target network command NAS message includes:

- Redirection validity indication: N/A
- Preferred network type: SNPN
- Ordered list of target network ID: SNPN-ID 1, SNPN-ID 2, SNPN-ID 3, …, etc.

For example, for steering the UE to an ordered list of preferred PLMNs case with redirection validity indication of a specific time and application ID, the UE may present to the users for manual selection of SNPNs or performs automatic SNPN selections for the user when the validity indication for time is met and the user is using the application, in which the redirect target network command NAS message includes:

- Redirection validity indication: validity time duration, application ID#1
- Preferred network type: PLMN
- Ordered list of target network ID: PLMN-ID 1, PLMN-ID 2, PLMN-ID 3, …, etc.

An example detailed solution for UE performing network re-selection procedure for both of PLMN and SNPN may be seen below with respect to solution 3.

**Solution 3: SOR support for both PLMN and SNPN**

Following solution 2, the SOR information may include additional information for guiding the UE to perform the network re-selection procedure. Solution 3 may involve one or more of the following Options:

<u>Option 1: SOR information adds a new IE to include a separate ordered list for the preferred SNPN-IDs (PLMN-ID + NPN-ID) and access technologies.</u>

- SNPN-ID list = {PLMN-ID 1+NPN-ID 1, PLMN-ID 2+NPN-ID 2, … , PLMN-ID k+NPN-ID k}
- This option assumes that the PALS SNPN network may use a specific set of mobile contruy code (MCC) identifiers (IDs) and mobile network code (MNC) IDs as a PLMN ID to indicate its usage as temporary access to local service at specific occasion, e.g. time and location.
- This option may support two separated network selection procedures based on an ordered list of the preferred PLMN ID and access technologies and another ordered list of the preferred PLMN ID and access technologies.

The SOR header includes a new IE for the indication of SNPN roaming preference. 0 represents PLMN preference and 1 represents SNPN preference.

- If this IE is set as 1, the UE performs SNPN selection procedure first based on the list of preferred SNPN ID and access technologies. If none of the SNPN is selected, the UE continues to perform PLMN selection procedure based on the list of preferred PLMN ID and access technologies.
- If this IE is set as 0, the UE performs PLMN selection procedure first based on the preferred PLMN ID and access technologies. If none of the PLMN is selected, the UE continues to perform SNPN selection procedure based on the list of preferred SNPN ID and access technologies.

Option 2: SOR information adds new IE to include a separate ordered list for the preferred NPN-IDs and access technologies.

- NPN-ID list = {NPN-ID 1, NPN-ID 2, … , NPN-ID k}
- This option may assume that the PALS SNPN network may use a dummy set of MCC ID and MNC ID as PLMN ID to indicate its usage as temporary access to local service at specific occasion, e.g. time and location.
- This option may support two separated network selection procedures based on an ordered list of the preferred PLMN ID and access technologies and another ordered list of the preferred PLMN ID and access technologies.

The SOR header includes a new IE for the indication of SNPN roaming preference. For example, 0 represents PLMN preference and 1 represents SNPN preference.

- If this IE is set as 1, the UE performs PLMN selection procedure first for discovering the PLMN-ID that is specifically for SNPN, e.g. dummy “999+MNC”. Based on the discovered SNPNs, the UE continue to perform SNPN selection procedure based on the list of preferred NPN ID and access technologies.
- If this IE is set as 0, the UE performs PLMN selection procedure first based on the preferred PLMN ID and access technologies. If none of the PLMN is selected, the UE continues to perform SNPN selection procedure based on the list of preferred NPN ID and access technologies.

Option 3: SOR information adds a new IE to include a separate ordered list for the preferred NPN-IDs and access technologies, and a separate ordered list for indicating the preferred network type.

- This option may support a unified network selection procedure by merging two ordered network lists including ordered list of the preferred PLMN ID and access technologies and another ordered list of the preferred PLMN ID and access technologies.
- Preferred network type is composed of 0, 1 sequence which indicates the order list for

the preferred network types in two lists. For example, the preferred network type indicates as (P, S, S, P, P, ...) which means the ordered list is (PLMN-ID 1, NPN-ID 1, NPN-ID 2, PLMN-ID 2, PLMN-ID 3, ...). Note that P represents PLMN and S represents SNPN in which P or S can be coded as 1 and 0.

- Alternatively, the list of preferred network types includes the pair of network type and the priority order in the corresponding network type. For example, the preferred network type indications as { (P, 1), (S, 1), (S, 2), (P, 2), ...} which means the ordered list is (PLMN-ID 1, NPN-ID 1, NPN-ID 2, PLMN-ID 2, PLMN-ID 3, ...).
- Alternatively, two different ordered lists for the preferred PLMN lists and ordered lists for the preferred SNPN lists are provided with relative priority indication for each entry. For example, preferred PLMN lists indicates as {(PLMN-ID 2, 3), (PLMN-ID 4, 1), ...} and preferred SNPN lists indicated as {(SNPN-ID 2, 2), (SNPN-ID 4, 4), ...}. The UE can interpretated the new ordered list as {PLMN-ID 4, SNPN-ID 2, PLMN-ID 2, SNPN-ID 4, ...}.
- Other implementations may be possible to compose the network list of SOR which contains both of PLMN and SNPN. Note that, as used herein, P represents PLMN and S represents SNPN in which P or S can be coded as 1 and 0.
- With the ordered list for the preferred network type, the UE can compose a new network list for performing network selection procedure based on the existing PLMN (re)-selection procedure.

The SOR header does not required the indication of PLMN and SNPN roaming preference.

In the case that the PALS SNPN network may use a specific set of MCC ID and MNC ID as PLMN ID to indicate its usage as temporary access to local service at specific occasion, e.g. time and location, a separate ordered list for the preferred SNPN-IDs (PLMN-ID + NPN-ID) and access technologies is provided in this option.

**Contextual Discussion**

The following includes excerpts from various 3GPP specifications. The excerpts may be from legacy specifications and highlight portions that are relevant to various solutions described herein and/or the excerpts may include proposed text of those specifications with updates in accordance with various embodiments.

3GPP TS 23.503:

Figures 5 and 6, which may be alternately viewed in 3GPP TS 23.503 illustrate examples of the overall architecture for policy and charging framework in the 5G system in both service-

based and reference point representation. Specifically, Figure 5 depicts an example of an overall non-roaming reference architecture of policy and charging control framework for the 5G System (service based representation), in accordance with various embodiments, and may correspond to 3GPP TS 23.503 Figure 5.2.1-1.

Figure 6 depicts an example of an overall non-roaming reference architecture of policy and charging control framework for the 5G System (reference point representation), in accordance with various embodiments, and may correspond to 3GPP TS 23.502 Figure 5.2.1-1a

3GPP TS 23.122, which may relate to solution 2, option 1 of this section

One purpose of the control plane solution for steering of roaming in 5GS procedure is to allow the HPLMN to update the "Operator Controlled PLMN Selector with Access Technology" list in the UE by providing the HPLMN protected list of preferred PLMN/access technology combinations via NAS signalling.

- If the selected PLMN is a VPLMN, the HPLMN can provide the steering of roaming information to the UE using the control plane mechanism during and after registration.
- If the selected PLMN is the HPLMN, the HPLMN can provide the steering of roaming information to the UE using the control plane mechanism after registration only.
- The HPLMN updates the "Operator Controlled PLMN Selector with Access Technology" based on the operator policies, which can be based on the registered VPLMN, the location of the UE, etc.

The HPLMN may configure their subscribed UE's universal mobile telecommunications service (UMTS) subscriber identity module (USIM) to indicate that the UE is expected to receive the steering of roaming information due to initial registration in a VPLMN.

- At the same time the HPLMN will mark the UE is expected to receive the steering of roaming information due to initial registration in a VPLMN, in the subscription information in the UDM.
- In this case, it is mandatory for the HPLMN to provide the steering of roaming information to the UE during initial registration in a VPLMN.
- Otherwise if such configuration is not provided in the USIM, it is optional for the HPLMN to provide the steering of roaming information to the UE during initial registration (based on operator policy).
- The HPLMN can provide the steering of roaming information to the UE during the registration procedure for mobility registration update and initial registration procedure for emergency services.
- In addition, the HPLMN can request the UE to provide an acknowledgement of successful

reception of the steering of roaming information.

NOTE 1: In annex C of the 3GPP TS 23.122, the User Data Repository (UDR) is considered as part of the UDM.

3GPP TS 24.501, which may relate to solution 3 of this section

*9.11.3.51 SOR transparent container*

One purpose of the SOR transparent container information element in the REGISTRATION ACCEPT message is to provide the list of preferred PLMN/access technology combinations (or HPLMN indication that 'no change of the "Operator Controlled PLMN Selector with Access Technology" list stored in the UE is needed and thus no list of preferred PLMN/access technology combinations is provided') (see 3GPP TS 23.122 annex C) and optional acknowledgement request.

One purpose of the SOR transparent container information element in the REGISTRATION COMPLETE message is to indicate the UE acknowledgement of successful reception of the SOR transparent container IE in the REGISTRATION ACCEPT message.

NOTE: When used in NAS transport procedure, the contents of the SOR transparent container information element in the Payload container IE of the DL NAS TRANSPORT message are used to provide the list of preferred PLMN/access technology combinations and optional acknowledgement request, and the contents of the SOR transparent container information element in the Payload container IE of the UL NAS TRANSPORT message are used to indicate the UE acknowledgement of successful reception of the SOR transparent container IE in the DL NAS TRANSPORT message.

The SOR transparent container information element is coded as shown in figure 9.11.3.51.1 [of 3GPP TS 24.501, depicted herein as Figure 7], figure 9.11.3.51.2 [of 3GPP TS 24.501, depicted herein as Figure 8], figure 9.11.3.51.3 [of 3GPP TS 24.501, depicted herein as Figure 9], figure 9.11.3.51.4 [of 3GPP TS 24.501, depicted herein as Figure 10], figure 9.11.3.51.5 [of 3GPP TS 24.501, depicted herein as Figure 11], figure 9.11.3.51.6 [of 3GPP TS 24.501, depicted herein as Figure 12] ,and table 9.11.3.51.1 [of TS 24.501, depicted below with 3GPP TS numbering].

The SOR transparent container is a type 6 information element with a minimum length of 20 octets.

**Table 9.11.3.51.1: SOR transparent container information element**

| |
|---|
| SOR-MAC-$I_{AUSF}$, SOR-MAC-$I_{UE}$ and $Counter_{SOR}$ are coded as specified in 3GPP TS 33.501 [24] |

SOR data type (octet 4, bit 1)

0 The SOR transparent container carries steering of roaming information.

1 The SOR transparent container carries acknowledgement of successful reception of the steering of roaming information.

List indication value (octet 4, bit 2)

0 HPLMN indication that 'no change of the "Operator Controlled PLMN Selector with Access Technology" list stored in the UE is needed and thus no list of preferred PLMN/access technology combinations is provided'

1 list of preferred PLMN/access technology combinations is provided

List type (octet 4, bit 3)

0 The list type is a secured packet.

1 The list type is a "PLMN ID and access technology list".

Acknowledgement (ACK) value (octet 4, bit 4)

0 acknowledgement not requested

1 acknowledgement requested

The secure packet is coded as specified in 3GPP TS 31.115 [22B].

The PLMN ID and access technology list consists of PLMN ID and access technology identifier and are coded as specified in 3GPP TS 31.102 [22] subclause 4.2.5. The PLMN ID and access technology identifier are provided in decreasing order of priority, e.g. PLMN ID 1 indicates highest priority and PLMN ID n indicates lowest priority.

3GPP TS 23.122, which may be related to solution 2, option 1 of this specification

*C.2 Stage-2 flow for steering of UE in VPLMN during registration*

The stage-2 flow for the case when the UE registers with VPLMN AMF is described below in figure C.2.1 [of 3GPP TS 23.122, depicted herein as Figures 13A and 13B]. The selected PLMN

is the VPLMN. The AMF is located in the selected VPLMN.

*C.3 Stage-2 flow for steering of UE in HPLMN or VPLMN after registration*

The stage-2 flow for the steering of UE in HPLMN or VPLMN after registration is indicated in figure C.3.1 [of 3GPP TS 32.122, depicted herein as Figure 14]. The selected PLMN can be the HPLMN or a VPLMN. The AMF is located in the selected PLMN. The flow is triggered:

- If the HPLMN UDM supports obtaining a list of preferred PLMN/access technology combinations or a secured packet from the SOR-AF, the HPLMN policy for the SOR-AF invocation is present in the HPLMN UDM and the SOR-AF provides the HPLMN UDM with a new list of preferred PLMN/access technology combinations or a secured packet for a UE identified by SUPI; or
- When a new list of preferred PLMN/access technology combinations or a secured packet becomes available in the HPLMN UDM.

NOTE: Before notifying the HPLMN UDM, the SOR-AF, based on operator policies or criteria, can obtain the user location information by triggering the unified location service exposure procedure as defined in 3GPP TS 23.273 [70] subclause 6.5, or additionally based on implementation specific criteria, by requesting the UE location information from other application function using implementation specific method. This user location information can then be used in the SOR-AF algorithms.

Security protection may be described, for example, in 3GPP TS 33.501.

3GPP TS 23.502 , which may be applicable to solution 2, option 2, and solution2.1)

*4.2.4.2 UE Configuration Update procedure for access and mobility management related parameters*

This procedure is initiated by the AMF when the AMF wants to update access and mobility management related parameters in the UE configuration.

This procedure is also used to trigger UE to perform, based on network indication, either Mobility Registration Update procedure while the UE is in CM-CONNECTED state to modify NAS parameters that require negotiation (e.g. MICO mode) or Mobility Registration Update procedure after the UE enters CM-IDLE state (e.g. for changes to Allowed NSSAI that require re-registration). If a Registration procedure is needed, the AMF provides an indication to the UE to initiate a Registration procedure.

UE Configuration Update shall be sent over the Access Type (e.g. 3GPP access or non-3GPP access) the UE Configuration Update is applied to, when applicable. If the AMF wants to

update NAS parameters in the UE which require UE acknowledgement, then the AMF provides an indication to the UE of whether the UE shall acknowledge the command or not. The AMF should not request acknowledgement of the NITZ command. The AMF shall request acknowledgement for NSSAI information (e.g. Allowed NSSAI), 5G-GUTI, TAI List, and Mobility Restrictions, LADN Information, MICO, Operator-defined access category definitions and SMS subscription.

[Figures 15A and 15B depict an example procedure as described herein. Specifically, Figures 15A and 15B depict Figure 4.2.4.2-1 of 3GPP TS 23.502]

0. AMF determines the necessity of UE configuration change due to various reasons (e.g. UE mobility change, NW policy, reception of Subscriber Data Update Notification from UDM, change of Network Slice configuration) or that the UE needs to perform a Registration Procedure. If a UE is in CM-IDLE, the AMF can wait until the UE is in CM-CONNECTED state or triggers Network Triggered Service Request (in clause 4.2.3.3).

NOTE 1: It is up to the network implementation whether the AMF can wait until the UE is in CM-CONNECTED state or trigger the Network Triggered Service Request.

NOTE 2: The AMF can check whether Network Slice configuration needs to be updated by using the Nnssf_NSSelection_Get service operation and in such case the AMF compares the stored information with the output from the NSSF to decide whether an update of the UE is required.

The AMF may include Mobility Restriction List in N2 message that delivers UE Configuration Update Command to the UE if the service area restriction for the UE is updated.

1. The AMF sends UE Configuration Update Command containing one or more UE parameters (Configuration Update Indication, 5G-GUTI, TAI List, Allowed NSSAI, Mapping Of Allowed NSSAI, Configured NSSAI for the Serving PLMN, Mapping Of Configured NSSAI, rejected S-NSSAIs, NITZ, Mobility Restrictions, LADN Information, MICO, Operator-defined access category definitions, SMS Subscribed Indication) to UE. Optionally, the AMF may update the rejected S-NSSAIs in the UE Configuration Update command.

The AMF includes one or more of 5G-GUTI, TAI List, Allowed NSSAI, Mapping Of Allowed NSSAI, Configured NSSAI for the Serving PLMN, Mapping Of Configured NSSAI, rejected S-NSSAIs, NITZ (Network Identity and Time Zone), Mobility Restrictions parameters, LADN Information, Operator-defined access category definitions or SMS Subscribed Indication if the AMF wants to update these NAS parameters without triggering a UE Registration procedure.

The AMF may include in the UE Configuration Update Command also Configuration Update Indication parameters indicating whether:

- Network Slicing Subscription Change has occurred;

- the UE shall acknowledge the command; and
- whether a Registration procedure is requested.

If the AMF indicates Network Slicing Subscription Change, then the UE shall locally erase all the network slicing configuration for all PLMNs and, if applicable, update the configuration for the current PLMN based on any received information. If the AMF indicates Network Slicing Subscription Change, the UE shall also be requested to acknowledge in step 2.

3GPP TS 23.502, which may be applicable to solution 2.2

*4.15.6.7 Service specific parameter provisioning (UE, UE Group, Any UE)*

This clause describes the procedures for enabling the AF to provide service specific parameters to 5G system via NEF.

The AF may issue requests on behalf of applications not owned by the PLMN serving the UE.

The AF request sent to the NEF contains the information as below:

**1)- Service Description.**

Service Description is the information to identify a service the Service Parameters are applied to.

The Service Description in the AF request can be represented by the combination of DNN and S-NSSAI, an AF-Service-Identifier or an application identifier.

**2) Service Parameters.**

Service Parameters are the service specific information which needs to be provisioned in the Network and delivered to the UE in order to support the service identified by the Service Description.

**3) Target UE(s) or a group of UEs. (optional)**

Target UE(s) or a group of UEs indicate the UE(s) who the Service Parameters shall be delivered to.

- Individual UEs can be identified by GPSI, or an IP address/Prefix or a MAC address.
- Groups of UEs can be identified by an External Group Identifiers as defined in TS 23.682 [23].
- If identifiers of target UE(s) or a group of UEs are not provided, then the Service Parameters shall be delived to any UEs using the service identified by the Service Description.

The NEF authorizes the AF request received from the AF and stores the information in the UDR as "Application Data". The Service Parameters are delivered to the targeted UE by the PCF when the UE is reachable.

Figure 4.15.6.7-1 [of 3GPP TS 23.402, depicted herein as Figure 4, described above]

shows procedure for service specific parameter provisioning.

- The AF uses Nnef_ServiceParameter service to provide the service specific parameters to the PLMN and the UE.

*4.2.4.3 UE Configuration Update procedure for transparent UE Policy delivery*

This procedure is initiated when the PCF wants to update UE access selection and PDU Session selection related policy information (e.g. UE policy) in the UE configuration. In the non-roaming case the V-PCF is not involved and the role of the H-PCF is performed by the PCF. For the roaming scenarios, the V-PCF interacts with the AMF and the H-PCF interacts with the V-PCF.

[Figure 16 an example procedure as described herein. Specifically, Figure 16 depicts Figure 4.2.4.3-1 of 3GPP TS 23.502]

0. PCF decides to update UE policy procedures based on triggering conditions such as an initial registration, or need for updating UE policy as follows:

- For initial registration case, the PCF compares the list of PSIs included in the UE access selection and PDU session selection related policy information in Npcf_UEPolicyControl_Create request and determine whether UE access selection and PDU Session selection related policy information have to be updated and be included in the answer to the AMF; and
- For the network triggered UE policy update case (e.g. the change of UE location, the change of Subscribed S-NSSAIs as described in clause 6.1.2.2.2 of TS 23.503 [20]), the PCF checks the latest list of PSIs to decide which UE access selection and/or PDU Session selection related policies have to be sent to the UE.

The PCF checks if the size of the resulting UE access selection and PDU Session selection related policy information exceeds a predefined limit:

- If the size is under the limit, then UE access selection and PDU Session selection related policy information are included in a single Namf_Communication_N1N2MessageTransfer service operation as described below.
- If the size exceeds the predefined limit, the PCF splits the UE access selection and PDU Session selection related policy information in smaller, logically independent UE access selection and PDU Session selection related policy information ensuring the size of each is under the predefined limit. Each UE access selection and PDU Session selection related policy information will be then sent in separated Namf_Communication_N1N2MessageTransfer service operations as described below.

NOTE 1: NAS messages from AMF to UE do not exceed the maximum size limit

allowed in NG-RAN (PDCP layer), so the predefined size limit in PCF is related to that limitation.

NOTE 2: The mechanism used to split the UE access selection and PDU Session selection related policy information is described in TS 29.507 [32].

1. PCF invokes Namf_Communication_N1N2MessageTransfer service operation provided by the AMF. The message includes SUPI, UE Policy Container.

2. If the UE is registered and reachable by AMF in either 3GPP access or non-3GPP access, AMF shall transfers transparently the UE Policy container to the UE via the registered and reachable access.

If the UE is registered in both 3GPP and non-3GPP accesses and reachable on both access and served by the same AMF, the AMF transfers transparently the UE Policy container to the UE via one of the accesses based on the AMF local policy.

If the UE is not reachable by AMF over both 3GPP access and non-3GPP access, the AMF reports to the PCF that the UE Policy container could not be delivered to the UE using Namf_Communication_N1N2TransferFailureNotification as in the step 5 in clause 4.2.3.3.

If AMF decides to transfer transparently the UE Policy container to the UE via 3GPP access, e.g. the UE is registered and reachable by AMF in 3GPP access only, or if the UE is registered and reachable by AMF in both 3GPP and non-3GPP accesses served by the same AMF and the AMF decides to transfer transparently the UE Policy container to the UE via 3GPP access based on local policy, and the UE is in CM-IDLE and reachable by AMF in 3GPP access, the AMF starts the paging procedure by sending a Paging message described in the step 4b of Network Triggered Service Request (in clause 4.2.3.3). Upon reception of paging request, the UE shall initiate the UE Triggered Service Request procedure (clause 4.2.3.2).

3. If the UE is in CM-CONNECTED over 3GPP access or non-3GPP access, the AMF transfers transparently the UE Policy container (UE access selection and PDU Session selection related policy information) received from the PCF to the UE. The UE Policy container includes the list of Policy Sections as described in TS 23.503 [20].

4. The UE updates the UE policy provided by the PCF and sends the result to the AMF.

5. If the AMF received the UE Policy container and the PCF subscribed to be notified of the reception of the UE Policy container then the AMF forwards the response of the UE to the PCF using Namf_N1MessageNotify.

The PCF maintains the latest list of PSIs delivered to the UE and updates the latest list of PSIs in the UDR by invoking Nudr_DM_Update (SUPI, Policy Data, Policy Set

Entry, updated PSI data) service operation.

**Mechanisms for Authentication and Authorization for Providing Access to Local Services in 5G Systems**

As previously noted, in 3GPP SA1, SP-200799 is a study item related to PALS. Various use cases are considered, which are not reiterated here for the sake of lack of redundancy. However, as noted, the use cases may need to enhance supports of a 5G network for UEs to access specific services offered by the service providers, including PLMN or NPN operator, or 3rd party service/content provider(s), via a 5G serving network in an on-demand, temporary basis and/or at specific location(s).

Embodiments herein provide example service requirements and solutions to address the following objective: Enabling access to the hosting network and specific services for users/UEs without previous relationship with the hosting network.

Based on use case 5.3 in 3GPP technical report (TR) 22.844, given an objective of PALS SID that UEs and their service providers are without a previous relationship to the hosting network for PALS service, automatic e-agreement mechanisms may be needed to allow network operators to build short term relationship using application layer approaches. The e-agreement mechanisms may allow the automation of multi-step processes in telecommunication domain to establish service level e-agreement among network operators for enabling the 5GS to facilitate the sharing of services and resources of the networks among network operators and to configure their networks and UEs accordingly for the PALS services at specific occasion, e.g. time and location. As shown in Figure 1, and as described above, the e-agreement may be established among service operators, e.g. SP-A, SP-B, and SP-C have no SLAs in place for the PALS services provided by SP-A's hosting network-A.

- The SP-A user/application may create an e-agreement that provides the PALS service configuration. The SP-B and SP-C users/application can subscribe this PALS service with required service policies for their UEs. The SP-B and SP-C can then configure their UEs for PALS service.
- Based on the PALS e-agreement, the hosting network may be configured with PALS service at a specific time and location for its PALS service subscribers (other network operator), e.g. PALS service policies of time, location, network-A access parameters, including spectrum, access technologies (3GPP or non-3GPP), network slice, charging policies, and subscriber's network policies for authentication, and routing.
- Based on the PALS e-agreement, the hosting network configuration creation and termination may be performed by SP-A or a trusted third-party application of the PALS

service subscriber representing other network operator. With the application layer approach, the PALS service can be used by authorized UEs of SP-A, SP-B, and SP-C which subscribes the PALS service.

With the e-agreement, the trust relationship among service providers may be assumed. Various embodiments herein provide solutions to ensure that the hosting network connectivity service is provided to an authenticated/authorized UEs in the following two scenarios in Figure 1:

- The UE accesses to hosting network (SP-A) for its home network services (SP-C)
- The UE accesses to hosting network (SP-A) for on demand services provided by the hosting network (SP-A) or other service providers (SP-B) that the UE does not have relationship with.

Embodiments in this section may include the following solutions and service requirements:

- Solution 4: federated identity provided by hosting network of SP-A
- Solution 5: User Identity/Credential for accessing hosting network connectivity services
- Solution 6: SoR (steering of roaming) and UE configuration for UE accessing the hosting network
- Solution 7: service requirements

For the sake of discussion of this section, the following assumptions may be made:

- An e-agreement is established for building the short-term relationship among service operators, e.g. SP-A, SP-B, and SP-C, which originally do not have SLAs in place for the PALS services provided by SP-A's hosting network-A.
- As shown in Figure 1, an automatic e-agreement mechanism is used to allow network operators, e.g. SP-A, SP-B, and SP-C, to build short term relationship using application layer approaches. The e-agreement mechanism allows the automation of multi-step processes in telecommunication domain to establish service level e-agreement among network operators for enabling the 5GS to facilitate the sharing of services and resources of the networks among network operators and to configure their networks and UEs accordingly for the PALS services at specific occasion, e.g. time and location.
- The UE's home network is SP-C and is regarded as a roaming UE by the hosting network of SP-A providing connectivity services.
- The UE accessing hosting network may be in the location within coverage of SP-A's network only, or coverage of both networks of SP-A and SP-C.

- UE ID is the 3GPP ID including international mobile subscriber identity (IMSI), subscription concealed identifier (SUCI), or subscription permanent identifier (SUPI).

Embodiments provide solutions to ensure that the hosting network providing 5G connectivity service is provided to an authenticated/authorized UEs in the following two scenarios in Figure 1:

- The UE accesses to hosting network (SP-A) for its home network services (SP-C)
- The UE accesses to hosting network (SP-A) for on demand services provided by the hosting network (SP-A) or other service providers (SP-B) that the UE does not have relationship with.

**Solution 4: federated identity provided by hosting network of SP-A**

With the e-agreement, the trust relationship among service providers can be assumed as shown in Figure 17 for the illustrative diagram of the relationship of security domains between hosting network (SP-A) and other service providers' network (SP-B, SP-C).

In the legacy mechanism in the evolved packet system (EPS)/5GS, the network operators manage user identities and subscriptions of their UE subscribers for home network services, e.g. SP-B and SP-C. In embodiments herein, for SP-A providing connectivity services via hosting network, the SP-A may also act as a user identity provider for the hosting network connectivity services based on the trust relationship established between SP-A and other service providers (SP-B and SP-C).

With the trusted SP-A acting as user identity provider (IdP), the SP-B as on-demand service provider can delegate authentication responsibility to SP-A for providing its on-demand services to other users that don't have relationship with SP-B. By this way, the UE of SP-C accessing the hosting network can use any on-demand services provided by the SP-A or other service providers, e.g. SP-B. The SP-A acting as user identity provider provides identity federation services to other service providers for serving their UEs.

Figure 18 depicts an example high level procedure of authentication/authorization of UE identities for the UE requesting to access home network services of SP-C and on-demand services of SP-A/SP-B via hosting network of SP-A, in which the UE has two different UE identities/credentials including UE-ID provided/managed by SP-C and UID (User Identifier) provided/managed by the hosting network of SP-A.

With respect to Figure 18, and for case (A): when the UE is in SP-C's network coverage and request to access services provided by SP-A's network:

- Step 1: the UE performs registration procedure using UE-ID of the SP-C, as indicated in 3GPP TS 23.502, clause 4.2.2.2, towards SP-C's network. The SP-C network performs

primary authentication based on UE-ID.

- Step 2: the user selects SP-A's service which triggers the UE to perform PDU session establishment request procedure using UID provided by SP-A, as indicated in 3GPP TS 23.502, clause 4.3.2.2, towards SP-C's network for SP-A's service.
- Step 3: SP-C initiates secondary authentication/authorization procedure towards entities, e.g. PDU session anchor (PSA) and DN-AAA, at SP-A based on the information of UID and network configuration information of the SP-A.

With respect to Figure 18, and for case (B): when the UE is in SP-A's network coverage and request to access to SP-A's network

- Step 0A: the UE is configured with access information for hosting network connectivity service

Step 0B: if step0A is not performed, the SP-A initiates this step after the UE registers to the SP-A to on boarding required information for UE accessing hosting network connectivity service.

- Step 1: the UE performs registration procedure using UE-ID of the SP-C and UID of the SP-A, as indicated in 3GPP TS 23.502, clause 4.2.2.2, towards SP-A's network.
- Step 2: the SP-A performs UID authentication and may determine to forward the authentication request message towards UE's home network of SP-C for primary authentication based on the information of UE-ID and network configuration information, e.g. UDM address, of SP-C. The primary authentication may be skipped by the SP-A if the registration of the UE is still valid.
    - If the primary authentication and UID authentication are both successful, the SP-A network establishes a default PDU session for the UE and presents on demand services via the portal websites to the UE.
- Step 3: the UE selects on demand services of the SP-B and performs PDU session establishment request procedure using UID of SP-A, as indicated in 3GPP TS 23.502, clause 4.3.2.2, towards SP-A's network for SP-B's on demand services.
- Step 4: based on the authentication/authorization policies of the on-demand services provided by the SP-B, the SP-A may determine to perform authentication of UID and request SP-B for service authorization indicating UID of the UE based on the network configuration info of SP-B network, e.g. PSA/DN-AAA for SP-B as network operator or Application server for SP-B as content provider. Alternatively, for SP-B as network operator, the SMF of the SP-A network forwards PDU session request indicating the results of the UID authentication towards SMF of the SP-B network for service authorization.

- Note that for UE's home network service of SP-C, the SP-A may apply the same authentication/authorization method as step3-step4 or use the existing roaming mechanism, e.g. forwards PDU session request towards UE's H-SMF of the SP-C.

In support of Case (B) scenario, the UE needs to be configured with information related to hosting network of SP-A by one or both of the following two techniques:

- Technique 1: using UE configuration procedure, as indicated in 3GPP TS 23.502, clause 4.2.4, initiated by the SP-C. (as indicated in Solution 5, step 6)
- Technique 2: using on boarding procedure to download the required UE configuration for SP-A access when the UE eligible for using SP-A services of the hosting network registers to SP-A but without related configuration. (as indicated in Solution 6)

For the charging aspects:

- For connectivity service at the hosting network, the SP-A network collects charging records for UE's usage of connectivity services at the hosting network.
- For on-demand services:
    - SP-B as network operator: the SP-B collects the charging record and report to SP-A for the usage of the on-demand services.
    - SP-B as content service provider: the SP-A may present the charging portal of SP-B to the UE for making the service payment and authorizing the service.
- The SP-A network provides the charging records for connectivity services and on demand services to UEs' home network of SP-C.

**Solution 5: User Identity/Credential for accessing hosting network connectivity services**

In this embodiment, the SP-A acting as user identity provider coordinates with other service providers, including network operator or content service provider, for generating user credentials for the eligible UE using hosting network connectivity for its home network services or on demand services. Figure 19 depicts an example in accordance with this embodiment. Specifically, Figure 19 depicts an example procedure for initiating hosting connectivity services for group users, in accordance with various embodiments. The example procedure may operate as follows:

Step 0 (not shown in Figure 19): When the e-agreement is established between SP-A and SP-C, the e-agreement includes the home network services for SP-C's subscribers and on-demand services for UEs of other service operators.

The SP-A manages the service subscription, which can be identified by SP identifier (SP-ID), of the SP-C and the SP-C obtains network configuration information, e.g. NEF of SP-A, AF

identifier and SP-ID of SP-C, which can be used by SP-C for provisioning services parameters to SP-A network via north bound APIs.

Step 1: AF of SP-C sends AF request message to request for user parameters for its subscriber using SP-A's connectivity services, in which AF request including the following information:

- AF identifier
- External identifier of SP-C
- PLMN ID if SP-C is MNO or PLMN ID plus NID if the SP-C is standalone NPN operator
- Group ID
- Number of UEs for the Group
- Service settings and parameters for the group:
    - Network parameters, e.g. QoS parameters, service function chaining settings, specific network resources (e.g., network slice).
    - Authentication/authorization policies for accessing home services via SP-A
    - Roaming configuration Data: UDM address, Home routing network configuration (H-SMF/PCF/UPF), Home Services DNN, S-NSSAI, provisioning server for on-boarding
    - On demand services settings provided by the SP-C: service descriptions, service authorization server configuration; DNN, S-NSSAI at the SP-C; charging policies
    - charging policies for the connectivity service via hosting network of SP-A

Step 2: the SP-A creates Group User profile for each Group of the SP-C which includes the Group ID and the following attributes:

- User credentials for accessing hosting network of SP-A, which are going to be used to authenticate a UE of SP-C which requesting for accessing hosting networks based on required number of UEs, in which the user credentials are created by the SP-A includes user identifier which may include the group ID information, and security keys, tokens, or certificates, based on the required UE capabilities of authentication, service group, etc.
- Unified Access Control (UAC) policy required for accessing hosting network
- Required UE capabilities for authentication,
- Authentication policies required by different services and slices to authenticate a UE in the group for accessing to the corresponding services or slices of the home network services.
- Specific service settings and parameters, including network parameters (e.g. QoS parameters, operator deployed service function chaining settings,

- Specific network access settings, e.g. DNN, network slices, allowable access technologies (3GPP access or non-3GPP access of Wifi).
- Validity condition of hosting network connectivity service of SP-A, e.g. time and location.
- Authorized on demand services provided by the SP-A or other service operators, e.g. SP-B.

Step 3: In response to AF request message, the NEF of SP-A provides AF response message including the following information per group:

- Group ID
- user credentials for accessing hosting network and using services via hosting network
- Required UE capabilities for authentication
- UAC policy, e.g. setting of access ID and/or one or more access categories
- SP-A network information for network selection, e.g. PLMN ID if SP-A is an MNO or SP-A's PLMN ID and NID (non public network ID) if SP-A is a Standalone Non public network operator.

Step 4: The SP-C manages the mapping between UE ID, group ID, and allocated user credential.

Step 5: The SP-C uses UE configuration update procedure, as indicated in TS23.502 clause 4.2.4 to configures its UE subscribers with at least one of the following information for accessing the SP-A's network:

- User credential including user identifier (UID), group ID if not as part of UID, security keys, token, certificates, etc. for SP-A services
- Required UE capabilities of authentication
- UAC policy, e.g. SP-A's access category
- Network ID of SP-A, e.g. PLMN ID or PLMN ID+NID

Step 6 (not shown in Figure 19): The UE selects SP-A network and requests to register to SP-A's network in which the registration request message includes UE-ID, UID, and group ID (if not as part of UID), the SP-A network forwards authentication request to SP-C and gets result of the UE authentication.

Step 7 (not shown in Figure 19): The SP-A network creates user context for the UE which includes user identifier and attributes of the associated service group.

**Solution 6: SoR and UE configuration for the hosting network**

Following solution 4, in support of Case (B) scenario, the UE needs to be configured with information related to hosting network of SP-A by one or both of the following two techniques:

- Technique 1: using UE configuration procedure, as indicated in 3GPP TS 23.502, clause 4.2.4, initiated by the SP-C. The details is in Solution 5, step 5.
- Technique 2: using on boarding procedure to download the required UE configuration for SP-A access when the UE eligible for using SP-A services of the hosting network registers to SP-A but without related configuration.

The UE configuration information includes:

- User credential including user identifier (UID), group ID if not as part of UID, security keys, token, certificates, etc. for SP-A services
- Required UE capabilities of authentication
- UAC policy, e.g. SP-A's access category
- Network ID of SP-A, e.g. PLMN ID or PLMN ID+NID

The technique 2 addresses the cases that a UE selects the hosting network of SP-A without pre-configuration of connectivity services provided by the hosting network, e.g. the UE manually selects the hosting network, the hosting network is the only available network around, etc. The technique 2 may follow one or more of the following steps:

- Step 1: the hosting network broadcasts the network ID of the service operators which have e-agreement for the hosting network connectivity services of SP-A, in which the network ID of SP-C can be PLMN-ID if SP-C is the MNO or PLMN-ID and NID if SP- is the standalone NPN (SNPN) operator.
- Step 2: the UE selects the cell broadcasting a network ID that matches its home network ID, and sends registration request message indicating its UE-ID.
- Step 3: the AMF of the hosting network of SP-C forwards the authentication request indicating UE-ID to the home UDM of the UE in SP-C based on the network operator's information indicated in UE-ID.
- Step 4: if the authentication of UE-ID is successful, the home UDM of the UE in SP-C retrieves SoR (steering of routing) information for the UE and returns the SoR information in authentication response message to AMF.
- Step 5: the AMF sends the registration accept message indicating the SoR information, PDU session establishment indication and required DNN/S-NSSAI of the PDU session, and on boarding server information to the UE.
- Step 6: the UE initiates the PDU session establishment procedure indicating the on boarding DNN/S-NSSAI and connects to the on boarding server of the SP-C to start on boarding the UE with the information related to one or more hosting network services at the location of the UE, e.g. the on boarding UE configuration may not limit to the UE configuration of SP-A in the case there are more hosting networks of different service

providers.

- Step 7: the UE may determine to initiate the PLMN/SNPN re-selection procedure based on the received on boarding information and SoR information.

**Solution 7: Service requirements**

The following describes different service requirements herein.

PALS service: a local connectivity service provided by a network operator for non-subscribers to access their desired services in a specific occasion, e.g. time and location.

PALS network: a 5G network which operator has temporary relationship and PALS service agreements with other network operators for providing PALS service to their subscribers as roaming UEs in a specific occasion, e.g. time and location.

In embodiments described herein, PALS network may be a hosting network and SP-A's network. Based on operator policies in e-agreement, the PALS network shall be able to authenticate a roaming UE using UE's credentials provided by its home operator when the roaming UE requests to use the PALS network for its home network services. The PALS network operator shall be able to act as an identity provider to provide user credentials for a roaming UE to access PALS network. The PALS network shall be able to authenticate the users using the configured credentials when the users of the roaming UEs request for on-demand services provided by the PALS network operator or other service providers.

**Contextual Discussion**

The following includes excerpts from various 3GPP specifications. The excerpts may be from legacy specifications and highlight portions that are relevant to various solutions described herein and/or the excerpts may include proposed text of those specifications with updates in accordance with various embodiments.

3GPP TS 23.503:

Figures 5 and 6, above, from 3GPP TS 23.503 illustrates the overall architecture for policy and charging framework in the 5G system in both service-based and reference point representation.

3GPP TS 23.502

*4.2.4 UE Configuration Update*

*4.2.4.1 General*

UE configuration may be updated by the network at any time using UE Configuration Update procedure. UE configuration includes:

- Access and Mobility Management related parameters decided and provided by the AMF. This includes the Configured NSSAI and its mapping to the Subscribed S-NSSAIs, the Allowed NSSAI and its mapping to Subscribed S-NSSAIs, the Service Gap time and the list of Rejected NSSAIs if the UE Configuration Update procedure is triggered by the AMF after Network Slice-Specific Authentication and Authorization of S-NSSAIs. If the UE and the AMF support RACS, this may also include a PLMN-assigned UE Radio Capability ID or alternatively a PLMN-assigned UE Radio Capability ID deletion indication.
- UE Policy provided by the PCF.

When AMF wants to change the UE configuration for access and mobility management related parameters the AMF initiates the procedure defined in clause 4.2.4.2. When the PCF wants to change or provide new UE Policies in the UE, the PCF initiates the procedure defined in clause 4.2.4.3 [of 3GPP TS 23.502].

If the UE Configuration Update procedure requires the UE to initiate a Registration procedure, the AMF indicates this to the UE explicitly.

4.2.4.2 UE Configuration Update procedure for access and mobility management related parameters

This procedure is initiated by the AMF when the AMF wants to update access and mobility management related parameters in the UE configuration. This procedure may be related to Figures 15A and 15B, as described above.

Clause 4.2.4.3: UE Configuration Update procedure for transparent UE Policy delivery

This procedure is initiated when the PCF wants to update UE access selection and PDU Session selection related policy information (e.g. UE policy) in the UE configuration. In the non-roaming case the V-PCF is not involved and the role of the H-PCF is performed by the PCF. For the roaming scenarios, the V-PCF interacts with the AMF and the H-PCF interacts with the V-PCF. This procedure may be related to Figure 16, described above.

**Mechanisms for Supporting Collaborative Romaing for Providing Access to Local Services in 5G Systems**

This section may relate to the solutions and requirements for considering interworking between Networks Operators and Application Providers for PALS. As previously discussed, the PALS may be provided at a specific occasion, e.g. time and location by the PALS network operator.

In 3GPP TS 22.278, Annex B1 provides various scenarios applicable for interworking between mobile operators and data applications for EPS and 5GS including:

- Operator owned non-roaming scenario
- Collaborative non-roaming scenario
- Operator owned/collaborative roaming scenario – Home Routed
- Collaborative roaming scenario – Local Breakout

Embodiments herein may extend the roaming scenarios applicable for interworking between PALS network operator and data applications based on service agreements for PALS services among network operators and application/service providers:

- PALS network operator owns the 5G network which provides access and IP connectivity to roaming UEs.
- Network operator owned application layer entities include Service Hosting Environment, and IMS network.
- Application platforms in third party domain can be owned by third party application/service providers, or home/other network operators.
- The Application platforms could be application servers (e.g. Video on Demand Server, Cloud gaming server, etc.), 3rd party software development platforms, and third party/operator Service Hosting Environments.

Figures 20 and 21 show the collaborative relationship in three domains including network operator providing access and IP connectivity, network operators providing services via IMS/application platforms, and application/service providers providing services via application platforms or applications. The dashed lines between PALS network operator and Home network operators are based on service level e-agreement and the horizontal line represents the demarcation between the network operator domains and the 3rd party domain. In an operator network, the application layer entities include IMS network, Application platforms, and API Gateway for third party applications developed using APIs (e.g. REST, GSMA OneAPI).

Figure 20 provides the home-routed roaming scenario for collaborative scenarios where traffic is routed to home network operator and applications are delivered by the home operator owned IMS or Application platform via roaming agreements between network operators.

Note: The other network operators and service/application operators in 3rd party domain provides collaborative services in application platforms to Home operator. The arrow solid line represents the traffic routed over trusted domains within home operator network while the arrow dash line represents the traffic routed over untrusted domain outside of home operator network.

Figure 21 provides the local breakout scenario for both owned and collaborative scenarios between PALS network operator and operators in 3rd party domains where traffic is routed to application from the PALS network to 1) PALS network owned application platforms, 2) collaborative home network owned application platforms, and 3) third parties via roaming agreements between PALS network operator and home/other network operators, and between PALS network operators and other application/service providers.

Note: The other network operators and application/service operators in 3rd party domain provides collaborative services in application platform to PALS network operator. The arrow solid lines represent the traffic routed over trusted domains within PALS network while the arrow dash lines represent the traffic routed over untrusted domain outside of PALS operator network.

In the case of the roaming for the local breakout scenario, the application platform may be owned by PALS network operator or collaborated with operators in 3rd party domains.

The PALS network routes the traffic to application from the PALS network to one or more of:

1) PALS network owned application platforms.
2) to a collaborative home network owned application platform.

to third parties via roaming agreements between PALS network operator and home/other network operators, and between PALS network operators and other application/service providers.

In the case of the roaming for home routed scenario, the application platform can be owned by home network operator or collaborated with operators in 3rd party domains.

The home routed roaming can be applied for one or more of:

- home operator owned services including IMS network, and service hosting environment (as known as Edge hosting environment or Edge Data Network).
- Collaborative services provided by third parties including other network operators owned IMS or application platform, or applications provided by services/application providers, which have service level agreements with home network operator.

The home routed roaming is to route the traffic towards a service hosting environment (application platform) owned by home network operator via routing interface between PALS network and home network or via local break out interface from PALS network toward data network. The roaming policies for home routed roaming or local breakout roaming may be provisioned by the

home network operator to PALS network via standardized APIs and the roaming policies are for an application, a group of applications, a data network, or network slices.

Example Techniques

Figure 22 depicts an example technique 2200 related to roaming between public and non-public 5G networks, in accordance with various embodiments. The technique 2200 may be performed by an element of a core network of a 5G network. Such an element may be, for example, a UDM or UDR of an HPLMN of a UE of the 5G network. The technique 2200 may include identifying, at 2205, an AF request received from an AF or NEF of the core network. The technique 2200 may further include identifying, at 2210 based on the AF request, SOR information to be provided to the UE. The technique 2200 may further include facilitating, at 2215, provision of the SOR information to the UE.

Figure 23 depicts an alternative example technique 2300 related to roaming between public and non-public 5G networks, in accordance with various embodiments. The technique 2300 may be performed by an element of a home network of a UE in a 5G network. Such an element may be, for example, an AF of the home network. The technique 2300 may include identifying, at 2305, that the UE is to access a hosting network that provides access to localized services as a PALS network. Such a recognition may occur based on a request from the UE or during a UE registration procedure. The technique 2300 may further include identifying, at 2310, one or more authentication parameters related to the PALS network. The identification may occur based on a transmission of an AF request to an element of the PALS network such as an NEF, and a corresponding response from the NEF. The technique 2300 may further include providing, at 2315, the one or more authentication parameters to the UE.

It will be recognized that the techniques 2200 and 2300 are intended as example techniques in accordance with some embodiments, and other embodiments may vary. For example, other techniques may include more or fewer elements, elements arranged in a different order than depicted, different elements, etc.

## SYSTEMS AND IMPLEMENTATIONS

Figures 24-25 illustrate various systems, devices, and components that may implement aspects of disclosed embodiments.

Figure 24 illustrates a network 2400 in accordance with various embodiments. The network 2400 may operate in a manner consistent with 3GPP technical specifications for LTE or 5G/NR systems. However, the example embodiments are not limited in this regard and the described embodiments may apply to other networks that benefit from the principles described herein, such as future 3GPP systems, or the like.

The network 2400 may include a UE 2402, which may include any mobile or non-mobile computing device designed to communicate with a RAN 2404 via an over-the-air connection. The UE 2402 may be communicatively coupled with the RAN 2404 by a Uu interface. The UE 2402 may be, but is not limited to, a smartphone, tablet computer, wearable computer device, desktop computer, laptop computer, in-vehicle infotainment, in-car entertainment device, instrument cluster, head-up display device, onboard diagnostic device, dashtop mobile equipment, mobile data terminal, electronic engine management system, electronic/engine control unit, electronic/engine control module, embedded system, sensor, microcontroller, control module, engine management system, networked appliance, machine-type communication device, M2M or D2D device, IoT device, etc.

In some embodiments, the network 2400 may include a plurality of UEs coupled directly with one another via a sidelink interface. The UEs may be M2M/D2D devices that communicate using physical sidelink channels such as, but not limited to, PSBCH, PSDCH, PSSCH, PSCCH, PSFCH, etc.

In some embodiments, the UE 2402 may additionally communicate with an AP 2406 via an over-the-air connection. The AP 2406 may manage a WLAN connection, which may serve to offload some/all network traffic from the RAN 2404. The connection between the UE 2402 and the AP 2406 may be consistent with any IEEE 802.11 protocol, wherein the AP 2406 could be a wireless fidelity (Wi-Fi®) router. In some embodiments, the UE 2402, RAN 2404, and AP 2406 may utilize cellular-WLAN aggregation (for example, LWA/LWIP). Cellular-WLAN aggregation may involve the UE 2402 being configured by the RAN 2404 to utilize both cellular radio resources and WLAN resources.

The RAN 2404 may include one or more access nodes, for example, AN 2408. AN 2408 may terminate air-interface protocols for the UE 2402 by providing access stratum protocols including RRC, PDCP, RLC, MAC, and L1 protocols. In this manner, the AN 2408 may enable data/voice connectivity between CN 2420 and the UE 2402. In some embodiments, the AN 2408

may be implemented in a discrete device or as one or more software entities running on server computers as part of, for example, a virtual network, which may be referred to as a CRAN or virtual baseband unit pool. The AN 2408 be referred to as a BS, gNB, RAN node, eNB, ng-eNB, NodeB, RSU, TRxP, TRP, etc. The AN 2408 may be a macrocell base station or a low power base station for providing femtocells, picocells or other like cells having smaller coverage areas, smaller user capacity, or higher bandwidth compared to macrocells.

In embodiments in which the RAN 2404 includes a plurality of ANs, they may be coupled with one another via an X2 interface (if the RAN 2404 is an LTE RAN) or an Xn interface (if the RAN 2404 is a 5G RAN). The X2/Xn interfaces, which may be separated into control/user plane interfaces in some embodiments, may allow the ANs to communicate information related to handovers, data/context transfers, mobility, load management, interference coordination, etc.

The ANs of the RAN 2404 may each manage one or more cells, cell groups, component carriers, etc. to provide the UE 2402 with an air interface for network access. The UE 2402 may be simultaneously connected with a plurality of cells provided by the same or different ANs of the RAN 2404. For example, the UE 2402 and RAN 2404 may use carrier aggregation to allow the UE 2402 to connect with a plurality of component carriers, each corresponding to a Pcell or Scell. In dual connectivity scenarios, a first AN may be a master node that provides an MCG and a second AN may be secondary node that provides an SCG. The first/second ANs may be any combination of eNB, gNB, ng-eNB, etc.

The RAN 2404 may provide the air interface over a licensed spectrum or an unlicensed spectrum. To operate in the unlicensed spectrum, the nodes may use LAA, eLAA, and/or feLAA mechanisms based on CA technology with PCells/Scells. Prior to accessing the unlicensed spectrum, the nodes may perform medium/carrier-sensing operations based on, for example, a listen-before-talk (LBT) protocol.

In V2X scenarios the UE 2402 or AN 2408 may be or act as a RSU, which may refer to any transportation infrastructure entity used for V2X communications. An RSU may be implemented in or by a suitable AN or a stationary (or relatively stationary) UE. An RSU implemented in or by: a UE may be referred to as a “UE-type RSU”; an eNB may be referred to as an “eNB-type RSU”; a gNB may be referred to as a “gNB-type RSU”; and the like. In one example, an RSU is a computing device coupled with radio frequency circuitry located on a roadside that provides connectivity support to passing vehicle UEs. The RSU may also include internal data storage circuitry to store intersection map geometry, traffic statistics, media, as well as applications/software to sense and control ongoing vehicular and pedestrian traffic. The RSU may provide very low latency communications required for high speed events, such as crash avoidance, traffic warnings, and the like. Additionally or alternatively, the RSU may provide other

cellular/WLAN communications services. The components of the RSU may be packaged in a weatherproof enclosure suitable for outdoor installation, and may include a network interface controller to provide a wired connection (e.g., Ethernet) to a traffic signal controller or a backhaul network.

In some embodiments, the RAN 2404 may be an LTE RAN 2410 with eNBs, for example, eNB 2412. The LTE RAN 2410 may provide an LTE air interface with the following characteristics: SCS of 15 kHz; CP-OFDM waveform for DL and SC-FDMA waveform for UL; turbo codes for data and TBCC for control; etc. The LTE air interface may rely on CSI-RS for CSI acquisition and beam management; PDSCH/PDCCH DMRS for PDSCH/PDCCH demodulation; and CRS for cell search and initial acquisition, channel quality measurements, and channel estimation for coherent demodulation/detection at the UE. The LTE air interface may operating on sub-6 GHz bands.

In some embodiments, the RAN 2404 may be an NG-RAN 2414 with gNBs, for example, gNB 2416, or ng-eNBs, for example, ng-eNB 2418. The gNB 2416 may connect with 5G-enabled UEs using a 5G NR interface. The gNB 2416 may connect with a 5G core through an NG interface, which may include an N2 interface or an N3 interface. The ng-eNB 2418 may also connect with the 5G core through an NG interface, but may connect with a UE via an LTE air interface. The gNB 2416 and the ng-eNB 2418 may connect with each other over an Xn interface.

In some embodiments, the NG interface may be split into two parts, an NG user plane (NG-U) interface, which carries traffic data between the nodes of the NG-RAN 2414 and a UPF 2448 (e.g., N3 interface), and an NG control plane (NG-C) interface, which is a signaling interface between the nodes of the NG-RAN2414 and an AMF 2444 (e.g., N2 interface).

The NG-RAN 2414 may provide a 5G-NR air interface with the following characteristics: variable SCS; CP-OFDM for DL, CP-OFDM and DFT-s-OFDM for UL; polar, repetition, simplex, and Reed-Muller codes for control and LDPC for data. The 5G-NR air interface may rely on CSI-RS, PDSCH/PDCCH DMRS similar to the LTE air interface. The 5G-NR air interface may not use a CRS, but may use PBCH DMRS for PBCH demodulation; PTRS for phase tracking for PDSCH; and tracking reference signal for time tracking. The 5G-NR air interface may operating on FR1 bands that include sub-6 GHz bands or FR2 bands that include bands from 24.25 GHz to 52.6 GHz. The 5G-NR air interface may include an SSB that is an area of a downlink resource grid that includes PSS/SSS/PBCH.

In some embodiments, the 5G-NR air interface may utilize BWPs for various purposes. For example, BWP can be used for dynamic adaptation of the SCS. For example, the UE 2402 can be configured with multiple BWPs where each BWP configuration has a different SCS. When a BWP change is indicated to the UE 2402, the SCS of the transmission is changed as well.

Another use case example of BWP is related to power saving. In particular, multiple BWPs can be configured for the UE 2402 with different amount of frequency resources (for example, PRBs) to support data transmission under different traffic loading scenarios. A BWP containing a smaller number of PRBs can be used for data transmission with small traffic load while allowing power saving at the UE 2402 and in some cases at the gNB 2416. A BWP containing a larger number of PRBs can be used for scenarios with higher traffic load.

The RAN 2404 is communicatively coupled to CN 2420 that includes network elements to provide various functions to support data and telecommunications services to customers/subscribers (for example, users of UE 2402). The components of the CN 2420 may be implemented in one physical node or separate physical nodes. In some embodiments, NFV may be utilized to virtualize any or all of the functions provided by the network elements of the CN 2420 onto physical compute/storage resources in servers, switches, etc. A logical instantiation of the CN 2420 may be referred to as a network slice, and a logical instantiation of a portion of the CN 2420 may be referred to as a network sub-slice.

In some embodiments, the CN 2420 may be an LTE CN 2422, which may also be referred to as an EPC. The LTE CN 2422 may include MME 2424, SGW 2426, SGSN 2428, HSS 2430, PGW 2432, and PCRF 2434 coupled with one another over interfaces (or "reference points") as shown. Functions of the elements of the LTE CN 2422 may be briefly introduced as follows.

The MME 2424 may implement mobility management functions to track a current location of the UE 2402 to facilitate paging, bearer activation/deactivation, handovers, gateway selection, authentication, etc.

The SGW 2426 may terminate an S1 interface toward the RAN and route data packets between the RAN and the LTE CN 2422. The SGW 2426 may be a local mobility anchor point for inter-RAN node handovers and also may provide an anchor for inter-3GPP mobility. Other responsibilities may include lawful intercept, charging, and some policy enforcement.

The SGSN 2428 may track a location of the UE 2402 and perform security functions and access control. In addition, the SGSN 2428 may perform inter-EPC node signaling for mobility between different RAT networks; PDN and S-GW selection as specified by MME 2424; MME selection for handovers; etc. The S3 reference point between the MME 2424 and the SGSN 2428 may enable user and bearer information exchange for inter-3GPP access network mobility in idle/active states.

The HSS 2430 may include a database for network users, including subscription-related information to support the network entities' handling of communication sessions. The HSS 2430 can provide support for routing/roaming, authentication, authorization, naming/addressing resolution, location dependencies, etc. An S6a reference point between the HSS 2430 and the

MME 2424 may enable transfer of subscription and authentication data for authenticating/authorizing user access to the LTE CN 2420.

The PGW 2432 may terminate an SGi interface toward a data network (DN) 2436 that may include an application/content server 2438. The PGW 2432 may route data packets between the LTE CN 2422 and the data network 2436. The PGW 2432 may be coupled with the SGW 2426 by an S5 reference point to facilitate user plane tunneling and tunnel management. The PGW 2432 may further include a node for policy enforcement and charging data collection (for example, PCEF). Additionally, the SGi reference point between the PGW 2432 and the data network 24 36 may be an operator external public, a private PDN, or an intra-operator packet data network, for example, for provision of IMS services. The PGW 2432 may be coupled with a PCRF 2434 via a Gx reference point.

The PCRF 2434 is the policy and charging control element of the LTE CN 2422. The PCRF 2434 may be communicatively coupled to the app/content server 2438 to determine appropriate QoS and charging parameters for service flows. The PCRF 2432 may provision associated rules into a PCEF (via Gx reference point) with appropriate TFT and QCI.

In some embodiments, the CN 2420 may be a 5GC 2440. The 5GC 2440 may include an AUSF 2442, AMF 2444, SMF 2446, UPF 2448, NSSF 2450, NEF 2452, NRF 2454, PCF 2456, UDM 2458, and AF 2460 coupled with one another over interfaces (or "reference points") as shown. Functions of the elements of the 5GC 2440 may be briefly introduced as follows.

The AUSF 2442 may store data for authentication of UE 2402 and handle authentication-related functionality. The AUSF 2442 may facilitate a common authentication framework for various access types. In addition to communicating with other elements of the 5GC 2440 over reference points as shown, the AUSF 2442 may exhibit an Nausf service-based interface.

The AMF 2444 may allow other functions of the 5GC 2440 to communicate with the UE 2402 and the RAN 2404 and to subscribe to notifications about mobility events with respect to the UE 2402. The AMF 2444 may be responsible for registration management (for example, for registering UE 2402), connection management, reachability management, mobility management, lawful interception of AMF-related events, and access authentication and authorization. The AMF 2444 may provide transport for SM messages between the UE 2402 and the SMF 2446, and act as a transparent proxy for routing SM messages. AMF 2444 may also provide transport for SMS messages between UE 2402 and an SMSF. AMF 2444 may interact with the AUSF 2442 and the UE 2402 to perform various security anchor and context management functions. Furthermore, AMF 2444 may be a termination point of a RAN CP interface, which may include or be an N2 reference point between the RAN 2404 and the AMF 2444; and the AMF 2444 may be a termination point of NAS (N1) signaling, and perform NAS ciphering and integrity protection.

AMF 2444 may also support NAS signaling with the UE 2402 over an N3 IWF interface.

The SMF 2446 may be responsible for SM (for example, session establishment, tunnel management between UPF 2448 and AN 2408); UE IP address allocation and management (including optional authorization); selection and control of UP function; configuring traffic steering at UPF 2448 to route traffic to proper destination; termination of interfaces toward policy control functions; controlling part of policy enforcement, charging, and QoS; lawful intercept (for SM events and interface to LI system); termination of SM parts of NAS messages; downlink data notification; initiating AN specific SM information, sent via AMF 2444 over N2 to AN 2408; and determining SSC mode of a session. SM may refer to management of a PDU session, and a PDU session or "session" may refer to a PDU connectivity service that provides or enables the exchange of PDUs between the UE 2402 and the data network 2436.

The UPF 2448 may act as an anchor point for intra-RAT and inter-RAT mobility, an external PDU session point of interconnect to data network 2436, and a branching point to support multi-homed PDU session. The UPF 2448 may also perform packet routing and forwarding, perform packet inspection, enforce the user plane part of policy rules, lawfully intercept packets (UP collection), perform traffic usage reporting, perform QoS handling for a user plane (e.g., packet filtering, gating, UL/DL rate enforcement), perform uplink traffic verification (e.g., SDF-to-QoS flow mapping), transport level packet marking in the uplink and downlink, and perform downlink packet buffering and downlink data notification triggering. UPF 2448 may include an uplink classifier to support routing traffic flows to a data network.

The NSSF 2450 may select a set of network slice instances serving the UE 2402. The NSSF 2450 may also determine allowed NSSAI and the mapping to the subscribed S-NSSAIs, if needed. The NSSF 2450 may also determine the AMF set to be used to serve the UE 2402, or a list of candidate AMFs based on a suitable configuration and possibly by querying the NRF 2454. The selection of a set of network slice instances for the UE 2402 may be triggered by the AMF 2444 with which the UE 2402 is registered by interacting with the NSSF 2450, which may lead to a change of AMF. The NSSF 2450 may interact with the AMF 2444 via an N22 reference point; and may communicate with another NSSF in a visited network via an N31 reference point (not shown). Additionally, the NSSF 2450 may exhibit an Nnssf service-based interface.

The NEF 2452 may securely expose services and capabilities provided by 3GPP network functions for third party, internal exposure/re-exposure, AFs (e.g., AF 2460), edge computing or fog computing systems, etc. In such embodiments, the NEF 2452 may authenticate, authorize, or throttle the AFs. NEF 2452 may also translate information exchanged with the AF 2460 and information exchanged with internal network functions. For example, the NEF 2452 may translate between an AF-Service-Identifier and an internal 5GC information. NEF 2452 may also receive

information from other NFs based on exposed capabilities of other NFs. This information may be stored at the NEF 2452 as structured data, or at a data storage NF using standardized interfaces. The stored information can then be re-exposed by the NEF 2452 to other NFs and AFs, or used for other purposes such as analytics. Additionally, the NEF 2452 may exhibit an Nnef service-based interface.

The NRF 2454 may support service discovery functions, receive NF discovery requests from NF instances, and provide the information of the discovered NF instances to the NF instances. NRF 2454 also maintains information of available NF instances and their supported services. As used herein, the terms "instantiate," "instantiation," and the like may refer to the creation of an instance, and an "instance" may refer to a concrete occurrence of an object, which may occur, for example, during execution of program code. Additionally, the NRF 2454 may exhibit the Nnrf service-based interface.

The PCF 2456 may provide policy rules to control plane functions to enforce them, and may also support unified policy framework to govern network behavior. The PCF 2456 may also implement a front end to access subscription information relevant for policy decisions in a UDR of the UDM 2458. In addition to communicating with functions over reference points as shown, the PCF 2456 exhibit an Npcf service-based interface.

The UDM 2458 may handle subscription-related information to support the network entities' handling of communication sessions, and may store subscription data of UE 2402. For example, subscription data may be communicated via an N8 reference point between the UDM 2458 and the AMF 2444. The UDM 2458 may include two parts, an application front end and a UDR. The UDR may store subscription data and policy data for the UDM 2458 and the PCF 2456, and/or structured data for exposure and application data (including PFDs for application detection, application request information for multiple UEs 2402) for the NEF 2452. The Nudr service-based interface may be exhibited by the UDR 221 to allow the UDM 2458, PCF 2456, and NEF 2452 to access a particular set of the stored data, as well as to read, update (e.g., add, modify), delete, and subscribe to notification of relevant data changes in the UDR. The UDM may include a UDM-FE, which is in charge of processing credentials, location management, subscription management and so on. Several different front ends may serve the same user in different transactions. The UDM-FE accesses subscription information stored in the UDR and performs authentication credential processing, user identification handling, access authorization, registration/mobility management, and subscription management. In addition to communicating with other NFs over reference points as shown, the UDM 2458 may exhibit the Nudm service-based interface.

The AF 2460 may provide application influence on traffic routing, provide access to NEF, and interact with the policy framework for policy control.

In some embodiments, the 5GC 2440 may enable edge computing by selecting operator/3rd party services to be geographically close to a point that the UE 2402 is attached to the network. This may reduce latency and load on the network. To provide edge-computing implementations, the 5GC 2440 may select a UPF 2448 close to the UE 2402 and execute traffic steering from the UPF 2448 to data network 2436 via the N6 interface. This may be based on the UE subscription data, UE location, and information provided by the AF 2460. In this way, the AF 2460 may influence UPF (re)selection and traffic routing. Based on operator deployment, when AF 2460 is considered to be a trusted entity, the network operator may permit AF 2460 to interact directly with relevant NFs. Additionally, the AF 2460 may exhibit an Naf service-based interface.

The data network 2436 may represent various network operator services, Internet access, or third party services that may be provided by one or more servers including, for example, application/content server 2438.

Figure 25 schematically illustrates a wireless network 2500 in accordance with various embodiments. The wireless network 2500 may include a UE 2502 in wireless communication with an AN 2504. The UE 2502 and AN 2504 may be similar to, and substantially interchangeable with, like-named components described elsewhere herein.

The UE 2502 may be communicatively coupled with the AN 2504 via connection 2506. The connection 2506 is illustrated as an air interface to enable communicative coupling, and can be consistent with cellular communications protocols such as an LTE protocol or a 5G NR protocol operating at mmWave or sub-6GHz frequencies.

The UE 2502 may include a host platform 2508 coupled with a modem platform 2510. The host platform 2508 may include application processing circuitry 2512, which may be coupled with protocol processing circuitry 2514 of the modem platform 2510. The application processing circuitry 2512 may run various applications for the UE 2502 that source/sink application data. The application processing circuitry 2512 may further implement one or more layer operations to transmit/receive application data to/from a data network. These layer operations may include transport (for example UDP) and Internet (for example, IP) operations

The protocol processing circuitry 2514 may implement one or more of layer operations to facilitate transmission or reception of data over the connection 2506. The layer operations implemented by the protocol processing circuitry 2514 may include, for example, MAC, RLC, PDCP, RRC and NAS operations.

The modem platform 2510 may further include digital baseband circuitry 2516 that may implement one or more layer operations that are “below” layer operations performed by the protocol processing circuitry 2514 in a network protocol stack. These operations may include, for example, PHY operations including one or more of HARQ-ACK functions,

scrambling/descrambling, encoding/decoding, layer mapping/de-mapping, modulation symbol mapping, received symbol/bit metric determination, multi-antenna port precoding/decoding, which may include one or more of space-time, space-frequency or spatial coding, reference signal generation/detection, preamble sequence generation and/or decoding, synchronization sequence generation/detection, control channel signal blind decoding, and other related functions.

The modem platform 2510 may further include transmit circuitry 2518, receive circuitry 2520, RF circuitry 2522, and RF front end (RFFE) 2524, which may include or connect to one or more antenna panels 2526. Briefly, the transmit circuitry 2518 may include a digital-to-analog converter, mixer, intermediate frequency (IF) components, etc.; the receive circuitry 2520 may include an analog-to-digital converter, mixer, IF components, etc.; the RF circuitry 2522 may include a low-noise amplifier, a power amplifier, power tracking components, etc.; RFFE 2524 may include filters (for example, surface/bulk acoustic wave filters), switches, antenna tuners, beamforming components (for example, phase-array antenna components), etc. The selection and arrangement of the components of the transmit circuitry 2518, receive circuitry 2520, RF circuitry 2522, RFFE 2524, and antenna panels 2526 (referred generically as "transmit/receive components") may be specific to details of a specific implementation such as, for example, whether communication is TDM or FDM, in mmWave or sub-6 gHz frequencies, etc. In some embodiments, the transmit/receive components may be arranged in multiple parallel transmit/receive chains, may be disposed in the same or different chips/modules, etc.

In some embodiments, the protocol processing circuitry 2514 may include one or more instances of control circuitry (not shown) to provide control functions for the transmit/receive components.

A UE reception may be established by and via the antenna panels 2526, RFFE 2524, RF circuitry 2522, receive circuitry 2520, digital baseband circuitry 2516, and protocol processing circuitry 2514. In some embodiments, the antenna panels 2526 may receive a transmission from the AN 2504 by receive-beamforming signals received by a plurality of antennas/antenna elements of the one or more antenna panels 2526.

A UE transmission may be established by and via the protocol processing circuitry 2514, digital baseband circuitry 2516, transmit circuitry 2518, RF circuitry 2522, RFFE 2524, and antenna panels 2526. In some embodiments, the transmit components of the UE 2504 may apply a spatial filter to the data to be transmitted to form a transmit beam emitted by the antenna elements of the antenna panels 2526.

Similar to the UE 2502, the AN 2504 may include a host platform 2528 coupled with a modem platform 2530. The host platform 2528 may include application processing circuitry

2532 coupled with protocol processing circuitry 2534 of the modem platform 2530. The modem platform may further include digital baseband circuitry 2536, transmit circuitry 2538, receive circuitry 2540, RF circuitry 2542, RFFE circuitry 2544, and antenna panels 2546. The components of the AN 2504 may be similar to and substantially interchangeable with like-named components of the UE 2502. In addition to performing data transmission/reception as described above, the components of the AN 2508 may perform various logical functions that include, for example, RNC functions such as radio bearer management, uplink and downlink dynamic radio resource management, and data packet scheduling.

Figure 26 is a block diagram illustrating components, according to some example embodiments, able to read instructions from a machine-readable or computer-readable medium (e.g., a non-transitory machine-readable storage medium) and perform any one or more of the methodologies discussed herein. Specifically, Figure 26 shows a diagrammatic representation of hardware resources 2600 including one or more processors (or processor cores) 2610, one or more memory/storage devices 2620, and one or more communication resources 2630, each of which may be communicatively coupled via a bus 2640 or other interface circuitry. For embodiments where node virtualization (e.g., NFV) is utilized, a hypervisor 2602 may be executed to provide an execution environment for one or more network slices/sub-slices to utilize the hardware resources 2600.

The processors 2610 may include, for example, a processor 2612 and a processor 2614. The processors 2610 may be, for example, a central processing unit (CPU), a reduced instruction set computing (RISC) processor, a complex instruction set computing (CISC) processor, a graphics processing unit (GPU), a DSP such as a baseband processor, an ASIC, an FPGA, a radio-frequency integrated circuit (RFIC), another processor (including those discussed herein), or any suitable combination thereof.

The memory/storage devices 2620 may include main memory, disk storage, or any suitable combination thereof. The memory/storage devices 2620 may include, but are not limited to, any type of volatile, non-volatile, or semi-volatile memory such as dynamic random access memory (DRAM), static random access memory (SRAM), erasable programmable read-only memory (EPROM), electrically erasable programmable read-only memory (EEPROM), Flash memory, solid-state storage, etc.

The communication resources 2630 may include interconnection or network interface controllers, components, or other suitable devices to communicate with one or more peripheral devices 2604 or one or more databases 2606 or other network elements via a network 2608. For example, the communication resources 2630 may include wired communication components (e.g., for coupling via USB, Ethernet, etc.), cellular communication components, NFC components,

Bluetooth® (or Bluetooth® Low Energy) components, Wi-Fi® components, and other communication components.

Instructions 2650 may comprise software, a program, an application, an applet, an app, or other executable code for causing at least any of the processors 2610 to perform any one or more of the methodologies discussed herein. The instructions 2650 may reside, completely or partially, within at least one of the processors 2610 (e.g., within the processor's cache memory), the memory/storage devices 2620, or any suitable combination thereof. Furthermore, any portion of the instructions 2650 may be transferred to the hardware resources 2600 from any combination of the peripheral devices 2604 or the databases 2606. Accordingly, the memory of processors 2610, the memory/storage devices 2620, the peripheral devices 2604, and the databases 2606 are examples of computer-readable and machine-readable media.

For one or more embodiments, at least one of the components set forth in one or more of the preceding figures may be configured to perform one or more operations, techniques, processes, and/or methods as set forth in the example section below. For example, the baseband circuitry as described above in connection with one or more of the preceding figures may be configured to operate in accordance with one or more of the examples set forth below. For another example, circuitry associated with a UE, base station, network element, etc. as described above in connection with one or more of the preceding figures may be configured to operate in accordance with one or more of the examples set forth below in the example section.

**EXAMPLES**

Example 1 may include the method of steering of roaming for UEs to access local services in 5GS.

Example 2 may include the method of example 1 and/or some other example herein, whereby the method is for home network provider or visiting network to direct or steer UEs to a PALS network (SNPN or PLMN) based on the location, time, specific local services, application request, or load balancing.

Example 3 may include the method of example 2 and/or some other example herein, whereby the home network provider provides steering of roaming (SOR) information to UE based on AF request.

Example 4 may include the method of example 3 and/or some other example herein, whereby the AF request message contains SOR information, SOR update indication, application IDs associated for SOR update.

Example 5 may include the method of example 4 and/or some other example herein, whereby the SOR information includes Network type, e.g. PALS network that provides access

to PALS services (identified by the application ID), Ordered lists of preferred PLMN/SNPN network identities, SOR validity indication.

Example 6 may include the method of example 5 and/or some other example herein, whereby the 5G network update SOR information to the UE via DL NAS message, UE configuration command or UE policy container to UEs after UE registration.

Example 7 may include the method of example 6 and/or some other example herein, whereby the UE enforces the network (re)-selection when the SOR validity indication such as the application is active, and the UE is at the specific location where the PLMN/SNPN network is available within validity time.

Example 8 may include the method of example 7 and/or some other example herein, whereby the UE performs network re-selection based on the ordered list of PLMN ID, ordered list of SNPN/NPN ID, and SOR header.

Example 9 may include the method of example 8 and/or some other example herein, whereby the SOR header indicates network roaming preference which indicates PLMN, SNPN, or both.

Example 10 may include the method of example 9 and/or some other example herein, whereby the UE performs SNPN selection first if network roaming preference is set as SNPN.

Example 11 may include the method of example 10 and/or some other example herein, whereby the UE performs PLMN selection first if network roaming preference is set as PLMN.

Example 12 may include the method of example 11 and/or some other example herein, whereby the UE manages a merged ordered network ID list which includes both of PLMN ID and the NPN-ID for PLMN and SNPN based on two ordered list of preference PLMN list and preferred SNPN/NPN list.

Example 13 may include the method of example 4 and/or some other example herein, whereby AF request message also contains Desired Edge Data Network information, e.g. combination of DNN, S-NSSAI, and EDSP (edge data network service provider) for the applications, which is used for the applications indicating the supported EGSP for the list of the preferred PLMN/SNPN network which can be used by the UE during PDU session establishment procedure for selecting a proper EDSP by the SMF.

Example 14 may include a method comprising:

receiving an AF request; and

providing, to a UE, steering of roaming (SOR) information to a UE based on the AF request.

Example 15 may include the method of example 14 and/or some other example herein, whereby the AF request message includes one or more of SOR information, SOR update

indication, and/or application IDs associated with an SOR update.

Example 16 may include the method of example 15 and/or some other example herein, wherein the SOR information includes one or more of a Network type (e.g. PALS network that provides access to PALS services (may identified by the application ID)), one or more ordered lists of preferred PLMN/SNPN network identities, and/or an SOR validity indication.

Example 17 may include a method for enabling authentication and authorization for providing access to local services in a 5G network.

Example 18 may include the method of example 17 and/or some other example herein, whereby the 5G network is UE's home network and provides a UE configuration to the UE, wherein the UE configuration includes one or more of:

- User credential, e.g., including one or more of user identifier (UID), group ID if not as part of UID, security keys, token, certificates, etc. for accessing PALS network;
- Required UE capabilities of authentication;
- UAC policy, e.g. PALS network's access category; and/or
- Network ID of PALS network, e.g. PLMN ID or PLMN ID+NID

Example 19 may include the method of example 18 and/or some other example herein, whereby the UE configuration is provided by the UE's home network via UE configuration update procedure when the UE is registered.

Example 20 may include the method of example 18 and/or some other example herein, whereby the UE configuration is provided via the hosting PALS network when the UE eligible for using the hosting PALS network requests to register to PALS network but without related configuration.

Example 21 may include the method of example 17 and/or some other example herein, whereby the PALS network authenticates a roaming UE using UE's credentials provided by its home operator when the roaming UE requests to use the PALS network for its home network services.

Example 22 may include the method of example 17 and/or some other example herein, whereby the PALS network operator acting as an identity provider provide user credentials for a roaming UE to access PALS network.

Example 23 may include the method of example 22 and/or some other example herein, whereby the PALS network authenticate the users using the configured credentials when the users of the roaming UEs request for on-demand services provided by the PALS network operator or other service providers.

Example 24 may include the method of example 17 and/or some other example herein,

whereby the AF of UE's home network sends AF request message to request for user parameters for its subscriber using SP-A's connectivity services, in which AF request includes one or more of the following information: AF identifier, External identifier of UE's home network, PLMN ID if UE's home network operator is MNO or PLMN ID plus NID if the UE's home network operator is standalone NPN operator, Group ID, Number of UEs for the Group, and Service settings and parameters for the group.

Example 25 may include the method of example 24 and/or some other example herein, whereby the service setting and parameters for the group include one or more of: Network parameters, e.g. QoS parameters, service function chaining settings, specific network resources (e.g., network slice); Authentication/authorization policies for accessing home services via PALS network; Roaming configuration Data: UDM address, Home routing network configuration (H-SMF/PCF/UPF), Home Services DNN, S-NSSAI, provisioning server for on-boarding; On demand services settings provided by the UE's home network: service descriptions, service authorization server configuration; DNN, S-NSSAI at the UE's home network; charging policies; charging policies for the connectivity service via hosting network of PALS network.

Example 26 may include the method of example 25 and/or some other example herein, whereby the PALS network creates Group User profile for each Group of the UE's home network which includes the Group ID and one or more of the following attributes:

- User credentials for accessing hosting PALS network, which are going to be used to authenticate a UE of its home network which requesting for accessing hosting networks based on required number of UEs, in which the user credentials are created by the PALS network includes user identifier which may include the group ID information, and security keys, tokens, or certificates, based on the required UE capabilities of authentication, service group, etc.
- Unified Access Control (UAC) policy required for accessing hosting PALS network
- Required UE capabilities for authentication,
- Authentication policies required by different services and slices to authenticate a UE in the group for accessing to the corresponding services or slices of the home network services.
- Specific service settings and parameters, including network parameters (e.g. QoS parameters, operator deployed service function chaining settings,
- Specific network access settings, e.g. DNN, network slices, allowable access technologies (3GPP access or non-3GPP access of Wifi).

- Validity condition of hosting network connectivity service of PALS network, e.g. time and location.
- Authorized on demand services provided by the PALS network operator or other service operators.

Example 27 may include the method of examples 25 or 26 and/or some other example herein, whereby in respond to AF request message, the NEF of the PALS network provides AF response message including one or more of the following information per group:

- Group ID
- user credentials for accessing hosting network and using services via hosting network
- Required UE capabilities for authentication
- UAC policy, e.g. setting of access ID and/or one or more access categories
- SP-A network information for network selection, e.g. PLMN ID if PALS network operator is an MNO or PALS network operator's PLMN ID and NID (non public network ID) if PALS network operator is a Standalone Non public network operator.

Example 28 may include a method of supporting collaborative roaming for providing access to local services (PALS) in 5G system based on roaming policies for PALS service.

Example 29 may include the method of example 28, and/or some other example herein, whereby the roaming is for the local breakout scenario for both owned and collaborative scenarios between PALS network operator and operators in 3rd party domains.

Example 30 may include the method of example 29, and/or some other example herein, whereby the PALS network routes the traffic to application from the PALS network to 1) PALS network owned application platforms.

Example 31 may include the method of example 30, and/or some other example herein, whereby the PALS network routes the traffic to a collaborative home network owned application platform.

Example 32 may include the method of example 31, and/or some other example herein, whereby the PALS network routes the traffic to third parties via roaming agreements between PALS network operator and home/other network operators, and between PALS network operators and other application/service providers.

Example 33 may include the method of example 28, and/or some other example herein, whereby the roaming is for the home routed scenario for home operator owned services including IMS network, and service hosting environment (as known as Edge hosting environment or Edge Data Network).

Example 34 may include the method of example 33, and/or some other example herein, whereby the home routed roaming is to route the traffic towards an service hosting environment

(application platform) owned by home network operator via routing interface between PALS network and home network or via local break out interface from PALS network toward data network.

Example 35 may include the method of example 34 and/or example 32, and/or some other example herein, whereby the home network operator and the PALS network operator have service level agreements for PALS provided by the PALS network operator to UEs of home network operator.

Example 36 may include the method of example 35, and/or some other example herein, whereby the roaming policies for home routed roaming or local breakout roaming is provisioned by the home network operator to PALS network via standardized APIs.

Example 37 may include the method of example 36, and/or some other example herein, whereby the roaming policies are for an application, a group of applications, a data network, or network slices.

Example 38 may include the method of example 36, and/or some other example herein, whereby the PALS is provided via PALS network at a specific occasion, e.g. time and location.

Example 39 includes a method comprising: identifying, by an element of a core network of a fifth generation (5G) network, an application function (AF) request received from an AF or network exposure function (NEF) of the core network; identifying, by the element based on the AF request, steering of roaming (SOR) information to be provided to a user equipment (UE) of the 5G network; and facilitating, by the element, provision of the SOR information to the UE.

Example 40 includes the method of example 39, and/or some other example herein, SOR information relates to a change of the UE from a home public land mobile network (HPLMN) to a visited public land mobile network (VPLMN)

Example 41 includes the method of example 40, and/or some other example herein, wherein the element is a unified data management (UDM) element or a unified data repository (UDR) of the HPLMN.

Example 42 includes the method of example 39, and/or some other example herein, wherein the facilitating the provision of the SOR information includes providing, by the element, the SOR information to an access mobility function (AMF) of the 5G network.

Example 43 includes the method of example 42, and/or some other example herein, wherein the AMF is to forward the SOR information to the UE.

Example 44 includes the method of any of examples 39-43, and/or some other example herein, wherein the AF request includes one or more of SOR information, an SOR update indication, and application identifiers (IDs) associated with an SOR update.

Example 45 includes the method of example 44, and/or some other example herein,

wherein the SOR information includes one or more of a network type, one or more ordered lists of preferred public land mobile network (PLMN) or standalone non-public network (SNPN) network identities, and an SOR validity indication.

Example 46 includes the method of example 45, and/or some other example herein, wherein the SOR validity indication includes the application IDs, a validity time, and a validity location.

Example 47 includes the method of any of examples 39-43, and/or some other example herein, wherein the AF request is a Nnef_ServiceParameter_Create/Update/Delete request.

Example 48 includes the method of any of examples 39-43, and/or some other example herein, wherein the SOR information is to steer the UE to a hosting network that provides access to localized services as a PALS network.

Example 49 includes a method comprising: identifying, by an element of a home network of a user equipment (UE) in a fifth generation (5G) network, that the UE is to access a hosting network that provides access to localized services as a PALS network; identifying, by the element of the home network of the UE, one or more authentication parameters related to the PALS network; and providing, by the element of the home network, the one or more authentication parameters to the UE.

Example 50 includes the method of example 49, and/or some other example herein, wherein the one or more authentication parameters include a user credential, an indication of UE capabilities required by the PALS network, an indication of an access category of the PALS network, or a network identifier of the PALS network.

Example 51 includes the method of example 50, and/or some other example herein, wherein the user credential is a user identifier (UID), a group identifier (ID), a security key, a token, or a certificate related to the PALS network.

Example 52 includes the method of example 49, and/or some other example herein, wherein provision of the one or more authentication parameters by the home network is related to a UE configuration update procedure related to UE registration to the home network.

Example 53 includes the method of example 49, and/or some other example herein, wherein provision of the one or more authentication parameters by the PALS network is related to a request received from the UE related to access by the UE to the PALS network.

Example 54 includes the method of example 49, and/or some other example herein, wherein the element of the home network is an application function (AF) of the home network.

Example 55 includes the method of example any of examples 49-54, and/or some other example herein, wherein identifying the one or more authentication parameters related to the PALS network includes transmitting, by the element of the home network, an AF request

message to an element of the PALS network.

Example 56 includes the method of example 55, and/or some other example herein, wherein the AF request message includes one or more of an AF identifier (ID), an external ID of the home network, a public land mobile network (PLMN) ID of the home network operator, a group ID, and a number of UEs in a group related to the group ID.

Example 57 includes the method of example 55, and/or some other example herein, wherein the one or more authentication parameters are related to a group user profile related to a group of UEs in the home network.

Example 58 includes the method of example 55, and/or some other example herein, wherein the element of the PALS network is a network exposure function (NEF) of the PALS network.

Example Z01 may include an apparatus comprising means to perform one or more elements of a method described in or related to any of examples 1-58, or any other method or process described herein.

Example Z02 may include one or more non-transitory computer-readable media comprising instructions to cause an electronic device, upon execution of the instructions by one or more processors of the electronic device, to perform one or more elements of a method described in or related to any of examples 1-58, or any other method or process described herein.

Example Z03 may include an apparatus comprising logic, modules, or circuitry to perform one or more elements of a method described in or related to any of examples 1-58, or any other method or process described herein.

Example Z04 may include a method, technique, or process as described in or related to any of examples 1-58, or portions or parts thereof.

Example Z05 may include an apparatus comprising: one or more processors and one or more computer-readable media comprising instructions that, when executed by the one or more processors, cause the one or more processors to perform the method, techniques, or process as described in or related to any of examples 1-58, or portions thereof.

Example Z06 may include a signal as described in or related to any of examples 1-58, or portions or parts thereof.

Example Z07 may include a datagram, packet, frame, segment, protocol data unit (PDU), or message as described in or related to any of examples 1-58, or portions or parts thereof, or otherwise described in the present disclosure.

Example Z08 may include a signal encoded with data as described in or related to any of examples 1-58, or portions or parts thereof, or otherwise described in the present disclosure.

Example Z09 may include a signal encoded with a datagram, packet, frame, segment,

protocol data unit (PDU), or message as described in or related to any of examples 1-58, or portions or parts thereof, or otherwise described in the present disclosure.

Example Z10 may include an electromagnetic signal carrying computer-readable instructions, wherein execution of the computer-readable instructions by one or more processors is to cause the one or more processors to perform the method, techniques, or process as described in or related to any of examples 1-58, or portions thereof.

Example Z11 may include a computer program comprising instructions, wherein execution of the program by a processing element is to cause the processing element to carry out the method, techniques, or process as described in or related to any of examples 1-58, or portions thereof.

Example Z12 may include a signal in a wireless network as shown and described herein.

Example Z13 may include a method of communicating in a wireless network as shown and described herein.

Example Z14 may include a system for providing wireless communication as shown and described herein.

Example Z15 may include a device for providing wireless communication as shown and described herein.

Any of the above-described examples may be combined with any other example (or combination of examples), unless explicitly stated otherwise. The foregoing description of one or more implementations provides illustration and description, but is not intended to be exhaustive or to limit the scope of embodiments to the precise form disclosed. Modifications and variations are possible in light of the above teachings or may be acquired from practice of various embodiments.

## Abbreviations and Terminology

Unless used differently herein, terms, definitions, and abbreviations may be consistent with terms, definitions, and abbreviations defined in 3GPP TR 21.905 v16.0.0 (2019-06).

For the purposes of the present document, the following terms and definitions are applicable to the examples and embodiments discussed herein.

MCG or the PSCell of the SCG for DC operation; otherwise, the term “Special The term “circuitry” as used herein refers to, is part of, or includes hardware components such as an electronic circuit, a logic circuit, a processor (shared, dedicated, or group) and/or memory (shared, dedicated, or group), an Application Specific Integrated Circuit (ASIC), a field-programmable device (FPD) (e.g., a field-programmable gate array (FPGA), a programmable logic device (PLD), a complex PLD (CPLD), a high-capacity PLD (HCPLD), a structured

ASIC, or a programmable SoC), digital signal processors (DSPs), etc., that are configured to provide the described functionality. In some embodiments, the circuitry may execute one or more software or firmware programs to provide at least some of the described functionality. The term "circuitry" may also refer to a combination of one or more hardware elements (or a combination of circuits used in an electrical or electronic system) with the program code used to carry out the functionality of that program code. In these embodiments, the combination of hardware elements and program code may be referred to as a particular type of circuitry.

The term "processor circuitry" as used herein refers to, is part of, or includes circuitry capable of sequentially and automatically carrying out a sequence of arithmetic or logical operations, or recording, storing, and/or transferring digital data. Processing circuitry may include one or more processing cores to execute instructions and one or more memory structures to store program and data information. The term "processor circuitry" may refer to one or more application processors, one or more baseband processors, a physical central processing unit (CPU), a single-core processor, a dual-core processor, a triple-core processor, a quad-core processor, and/or any other device capable of executing or otherwise operating computer-executable instructions, such as program code, software modules, and/or functional processes. Processing circuitry may include more hardware accelerators, which may be microprocessors, programmable processing devices, or the like. The one or more hardware accelerators may include, for example, computer vision (CV) and/or deep learning (DL) accelerators. The terms "application circuitry" and/or "baseband circuitry" may be considered synonymous to, and may be referred to as, "processor circuitry."

The term "interface circuitry" as used herein refers to, is part of, or includes circuitry that enables the exchange of information between two or more components or devices. The term "interface circuitry" may refer to one or more hardware interfaces, for example, buses, I/O interfaces, peripheral component interfaces, network interface cards, and/or the like.

The term "user equipment" or "UE" as used herein refers to a device with radio communication capabilities and may describe a remote user of network resources in a communications network. The term "user equipment" or "UE" may be considered synonymous to, and may be referred to as, client, mobile, mobile device, mobile terminal, user terminal, mobile unit, mobile station, mobile user, subscriber, user, remote station, access agent, user agent, receiver, radio equipment, reconfigurable radio equipment, reconfigurable mobile device, etc. Furthermore, the term "user equipment" or "UE" may include any type of wireless/wired device or any computing device including a wireless communications interface.

The term "network element" as used herein refers to physical or virtualized equipment and/or infrastructure used to provide wired or wireless communication network services. The

term "network element" may be considered synonymous to and/or referred to as a networked computer, networking hardware, network equipment, network node, router, switch, hub, bridge, radio network controller, RAN device, RAN node, gateway, server, virtualized VNF, NFVI, and/or the like.

The term "computer system" as used herein refers to any type interconnected electronic devices, computer devices, or components thereof. Additionally, the term "computer system" and/or "system" may refer to various components of a computer that are communicatively coupled with one another. Furthermore, the term "computer system" and/or "system" may refer to multiple computer devices and/or multiple computing systems that are communicatively coupled with one another and configured to share computing and/or networking resources.

The term "appliance," "computer appliance," or the like, as used herein refers to a computer device or computer system with program code (e.g., software or firmware) that is specifically designed to provide a specific computing resource. A "virtual appliance" is a virtual machine image to be implemented by a hypervisor-equipped device that virtualizes or emulates a computer appliance or otherwise is dedicated to provide a specific computing resource.

The term "resource" as used herein refers to a physical or virtual device, a physical or virtual component within a computing environment, and/or a physical or virtual component within a particular device, such as computer devices, mechanical devices, memory space, processor/CPU time, processor/CPU usage, processor and accelerator loads, hardware time or usage, electrical power, input/output operations, ports or network sockets, channel/link allocation, throughput, memory usage, storage, network, database and applications, workload units, and/or the like. A "hardware resource" may refer to compute, storage, and/or network resources provided by physical hardware element(s). A "virtualized resource" may refer to compute, storage, and/or network resources provided by virtualization infrastructure to an application, device, system, etc. The term "network resource" or "communication resource" may refer to resources that are accessible by computer devices/systems via a communications network. The term "system resources" may refer to any kind of shared entities to provide services, and may include computing and/or network resources. System resources may be considered as a set of coherent functions, network data objects or services, accessible through a server where such system resources reside on a single host or multiple hosts and are clearly identifiable.

The term "channel" as used herein refers to any transmission medium, either tangible or intangible, which is used to communicate data or a data stream. The term "channel" may be synonymous with and/or equivalent to "communications channel," "data communications channel," "transmission channel," "data transmission channel," "access channel," "data access

channel," "link," "data link," "carrier," "radiofrequency carrier," and/or any other like term denoting a pathway or medium through which data is communicated. Additionally, the term "link" as used herein refers to a connection between two devices through a RAT for the purpose of transmitting and receiving information.

The terms "instantiate," "instantiation," and the like as used herein refers to the creation of an instance. An "instance" also refers to a concrete occurrence of an object, which may occur, for example, during execution of program code.

The terms "coupled," "communicatively coupled," along with derivatives thereof are used herein. The term "coupled" may mean two or more elements are in direct physical or electrical contact with one another, may mean that two or more elements indirectly contact each other but still cooperate or interact with each other, and/or may mean that one or more other elements are coupled or connected between the elements that are said to be coupled with each other. The term "directly coupled" may mean that two or more elements are in direct contact with one another. The term "communicatively coupled" may mean that two or more elements may be in contact with one another by a means of communication including through a wire or other interconnect connection, through a wireless communication channel or link, and/or the like.

The term "information element" refers to a structural element containing one or more fields. The term "field" refers to individual contents of an information element, or a data element that contains content.

The term "SMTC" refers to an SSB-based measurement timing configuration configured by *SSB-MeasurementTimingConfiguration*.

The term "SSB" refers to an SS/PBCH block.

The term "a "Primary Cell" refers to the MCG cell, operating on the primary frequency, in which the UE either performs the initial connection establishment procedure or initiates the connection re-establishment procedure.

The term "Primary SCG Cell" refers to the SCG cell in which the UE performs random access when performing the Reconfiguration with Sync procedure for DC operation.

The term "Secondary Cell" refers to a cell providing additional radio resources on top of a Special Cell for a UE configured with CA.

The term "Secondary Cell Group" refers to the subset of serving cells comprising the PSCell and zero or more secondary cells for a UE configured with DC.

The term "Serving Cell" refers to the primary cell for a UE in RRC_CONNECTED not configured with CA/DC there is only one serving cell comprising of the primary cell.

The term "serving cell" or "serving cells" refers to the set of cells comprising the Special

Cell(s) and all secondary cells for a UE in RRC_CONNECTED configured with CA/.

The term “Special Cell” refers to the PCell of the Cell” refers to the Pcell.

# CLAIMS

1. A method comprising:

identifying, by an element of a core network of a fifth generation (5G) network, an application function (AF) request received from an AF or network exposure function (NEF) of the core network;

identifying, by the element based on the AF request, steering of roaming (SOR) information to be provided to a user equipment (UE) of the 5G network; and

facilitating, by the element, provision of the SOR information to the UE.

2. The method of claim 1, SOR information relates to a change of the UE from a home public land mobile network (HPLMN) to a visited public land mobile network (VPLMN)

3. The method of claim 2, wherein the element is a unified data management (UDM) element or a unified data repository (UDR) of the HPLMN.

4. The method of claim 1, wherein the facilitating the provision of the SOR information includes providing, by the element, the SOR information to an access mobility function (AMF) of the 5G network.

5. The method of claim 4, wherein the AMF is to forward the SOR information to the UE.

6. The method of any of claims 1-5, wherein the AF request includes one or more of SOR information, an SOR update indication, and application identifiers (IDs) associated with an SOR update.

7. The method of claim 6, wherein the SOR information includes one or more of a network type, one or more ordered lists of preferred public land mobile network (PLMN) or standalone non-public network (SNPN) network identities, and an SOR validity indication.

8. The method of claim 7, wherein the SOR validity indication includes the application IDs, a validity time, and a validity location.

9. The method of any of claims 1-5, wherein the AF request is a

Nnef_ServiceParameter_Create/Update/Delete request.

10. The method of any of claims 1-5, wherein the SOR information is to steer the UE to a hosting network that provides access to localized services as a PALS network.

11. A method comprising:

identifying, by an element of a home network of a user equipment (UE) in a fifth generation (5G) network, that the UE is to access a hosting network that provides access to localized services as a PALS network;

identifying, by the element of the home network of the UE, one or more authentication parameters related to the PALS network; and

providing, by the element of the home network, the one or more authentication parameters to the UE.

12. The method of claim 11, wherein the one or more authentication parameters include a user credential, an indication of UE capabilities required by the PALS network, an indication of an access category of the PALS network, or a network identifier of the PALS network.

13. The method of claim 12, wherein the user credential is a user identifier (UID), a group identifier (ID), a security key, a token, or a certificate related to the PALS network.

14. The method of claim 11, wherein provision of the one or more authentication parameters by the home network is related to a UE configuration update procedure related to UE registration to the home network.

15. The method of claim 11, wherein provision of the one or more authentication parameters by the PALS network is related to a request received from the UE related to access by the UE to the PALS network.

16. The method of claim 11, wherein the element of the home network is an application function (AF) of the home network.

17. The method of any of claims 11-16, wherein identifying the one or more authentication parameters related to the PALS network includes transmitting, by the element of the home network, an AF request message to an element of the PALS network.

18. The method of claim 17, wherein the AF request message includes one or more of an AF identifier (ID), an external ID of the home network, a public land mobile network (PLMN) ID of the home network operator, a group ID, and a number of UEs in a group related to the group ID.

19. The method of claim 17, wherein the one or more authentication parameters are related to a group user profile related to a group of UEs in the home network.

20. The method of claim 17, wherein the element of the PALS network is a network exposure function (NEF) of the PALS network.

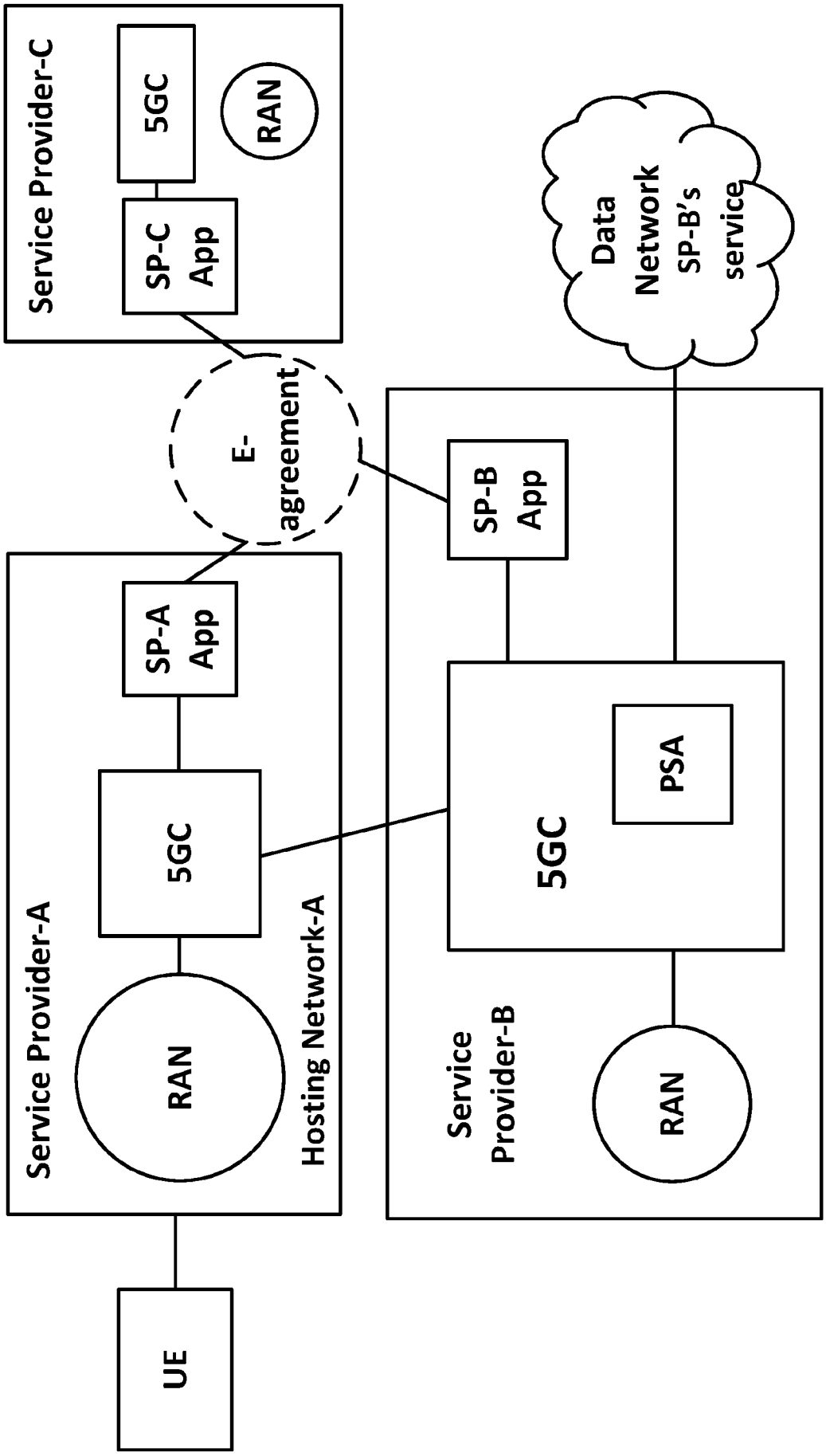
Service Provider-C
5GC
RAN
SP-C App
Data Network SP-B's service
E-agreement
SP-B App
SP-A App
5GC
PSA
Service Provider-A
Hosting Network-A
RAN
Service Provider-B
RAN
UE

Figure 1

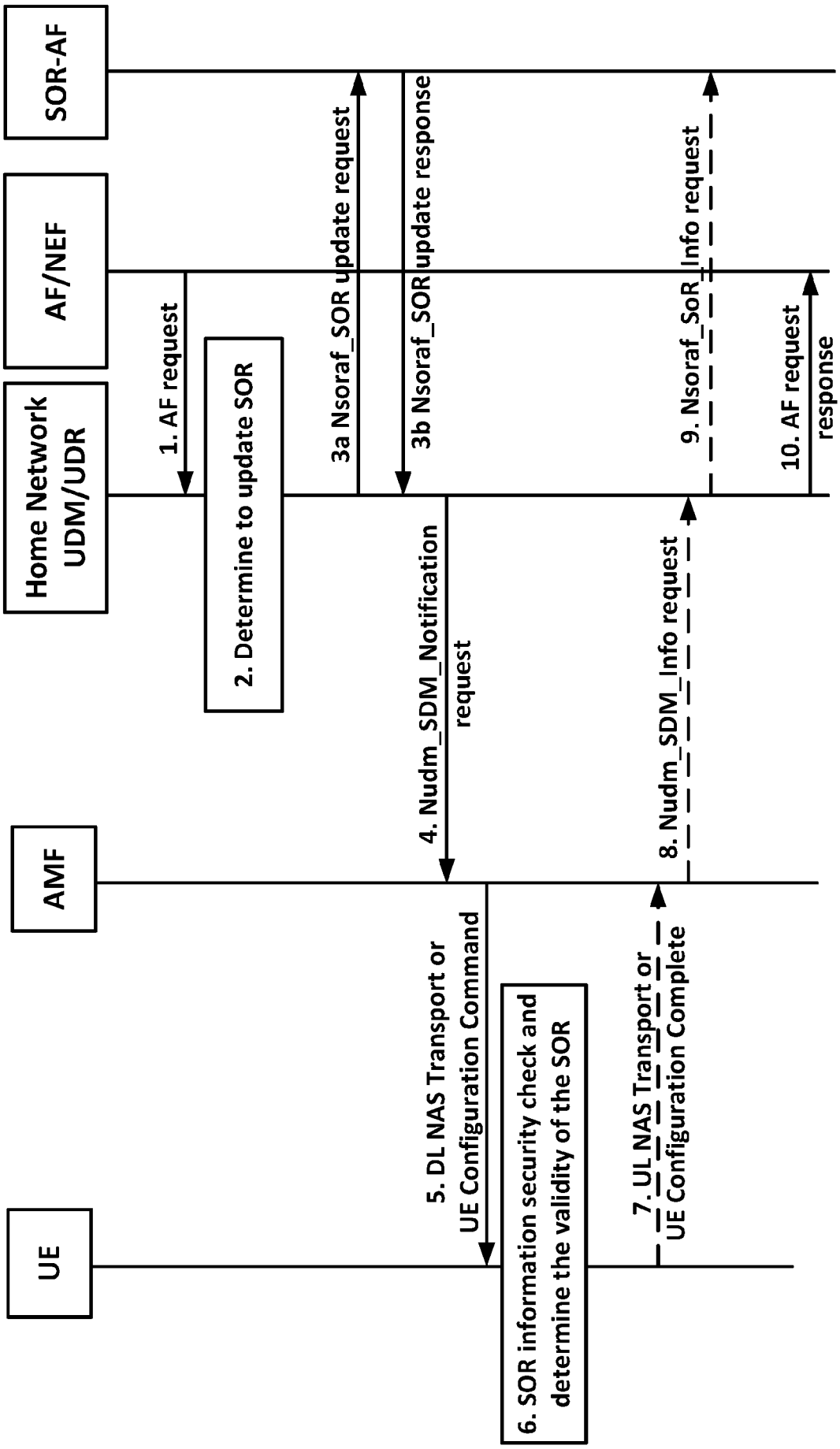
UE
AMF
Home Network UDM/UDR
AF/NEF
SOR-AF
1. AF request
2. Determine to update SOR
3a Nsoraf_SOR update request
3b Nsoraf_SOR update response
4. Nudm_SDM_Notification request
5. DL NAS Transport or UE Configuration Command
6. SOR information security check and determine the validity of the SOR
7. UL NAS Transport or UE Configuration Complete
8. Nudm_SDM_Info request
9. Nsoraf_SoR_Info request
10. AF request response

Figure 2

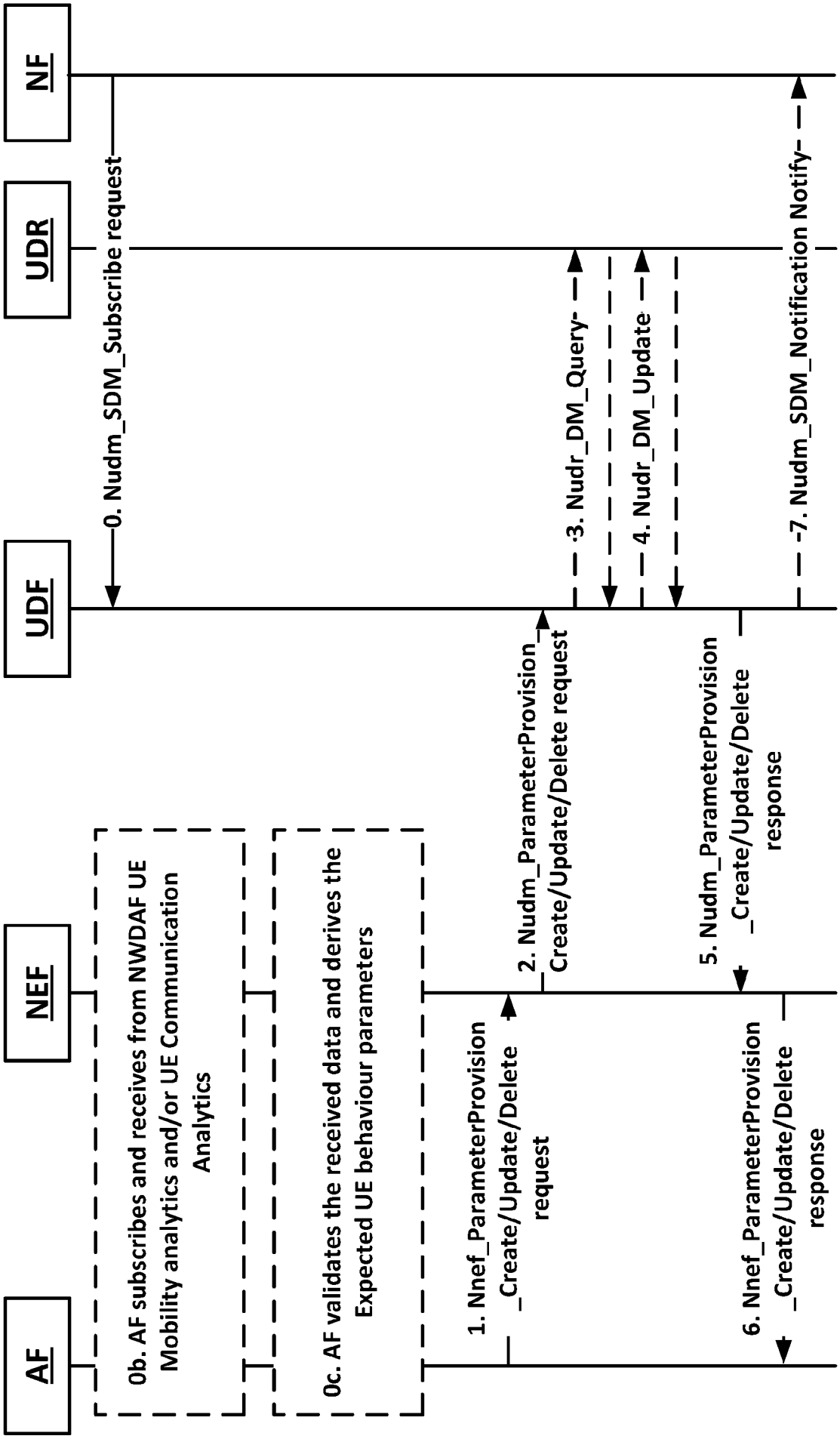
AF
NEF
UDF
UDR
NF
0. Nudm_SDM_Subscribe request
0b. AF subscribes and receives from NWDAF UE Mobility analytics and/or UE Communication Analytics
0c. AF validates the received data and derives the Expected UE behaviour parameters
1. Nnef_ParameterProvision _Create/Update/Delete request
2. Nudm_ParameterProvision Create/Update/Delete request
3. Nudr_DM_Query
4. Nudr_DM_Update
5. Nudm_ParameterProvision _Create/Update/Delete response
6. Nnef_ParameterProvision _Create/Update/Delete response
7. Nudm_SDM_Notification Notify

Figure 3

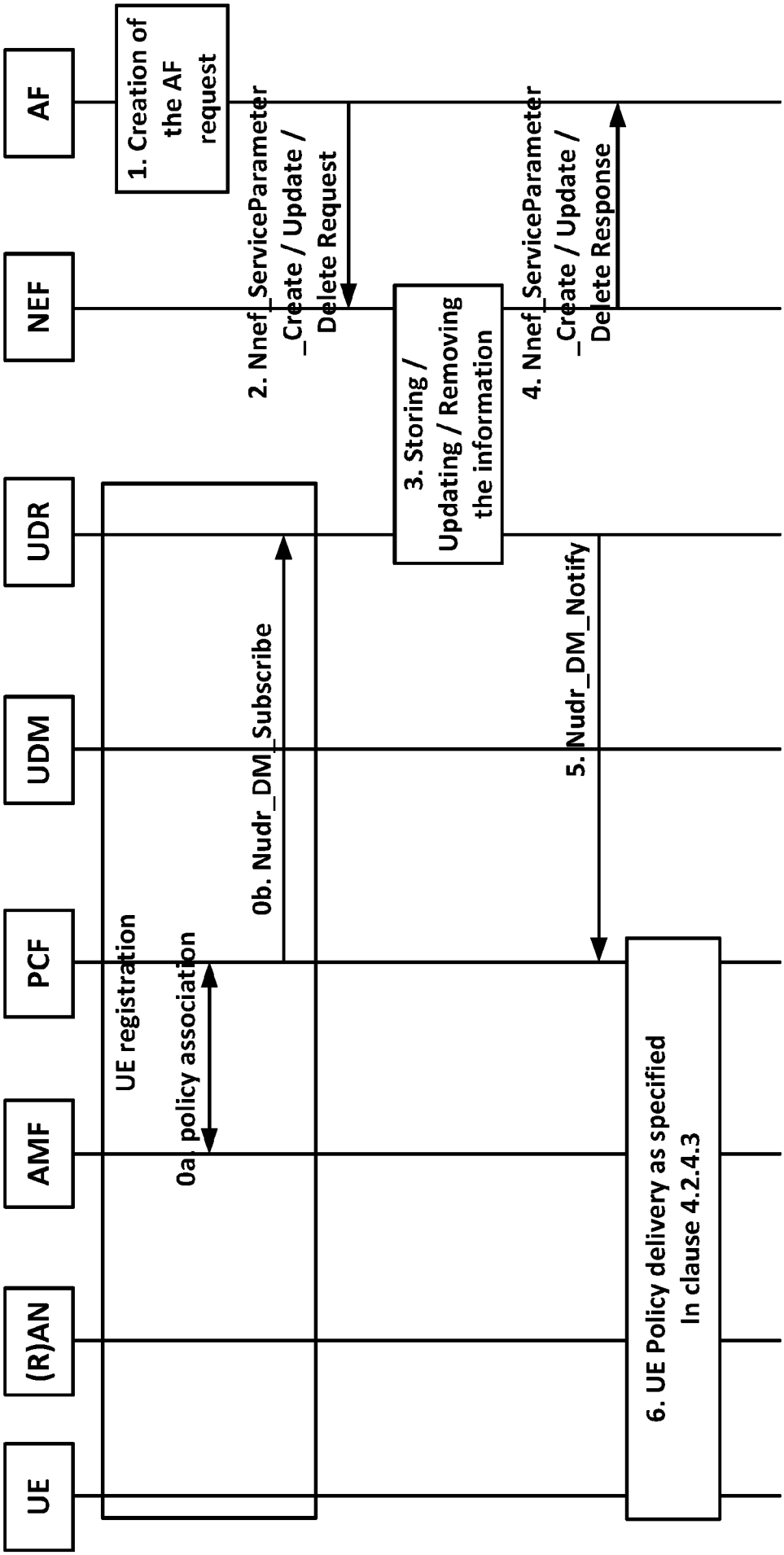
UE
(R)AN
AMF
PCF
UDM
UDR
NEF
AF
1. Creation of the AF request
2. Nnef_ServiceParameter _Create / Update / Delete Request
3. Storing / Updating / Removing the information
4. Nnef_ServiceParameter _Create / Update / Delete Response
5. Nudr_DM_Notify
0b. Nudr_DM_Subscribe
UE registration
0a. policy association
6. UE Policy delivery as specified In clause 4.2.4.3

Figure 4

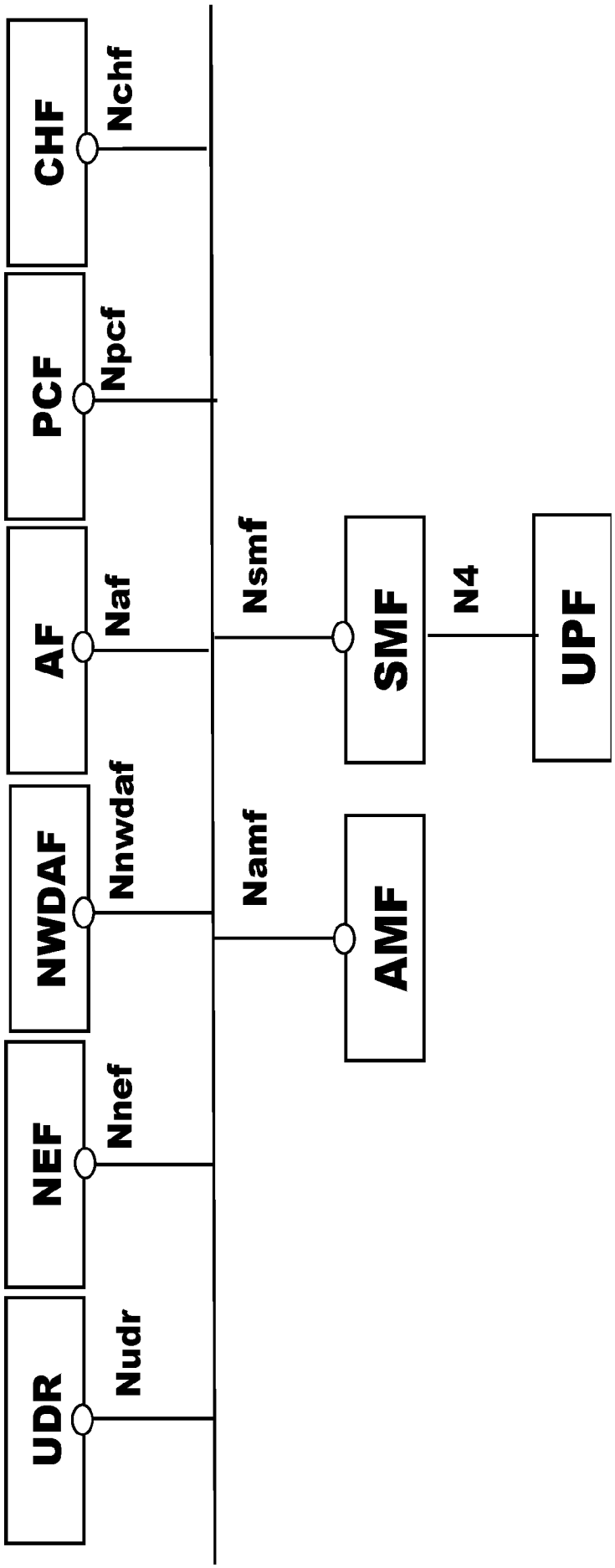
CHF
Nchf
PCF
Npcf
AF
Naf
NWDAF
Nnwdaf
NEF
Nnef
UDR
Nudr
Nsmf
Namf
SMF
AMF
N4
UPF

Figure 5

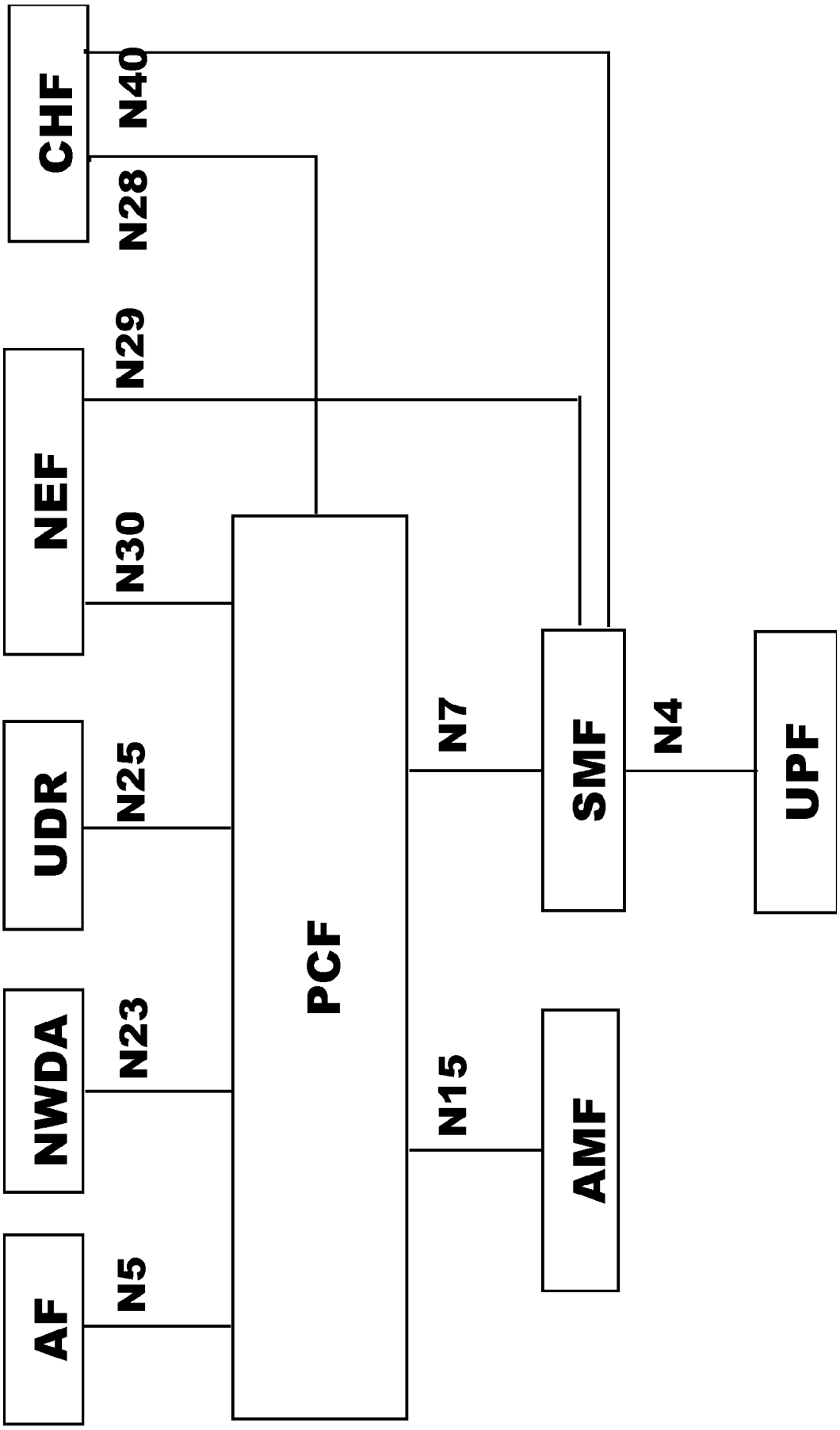
CHF
N40
N28
N29
NEF
N30
UDR
N25
NWDA
N23
AF
N5
PCF
N7
SMF
N4
UPF
N15
AMF

Figure 6

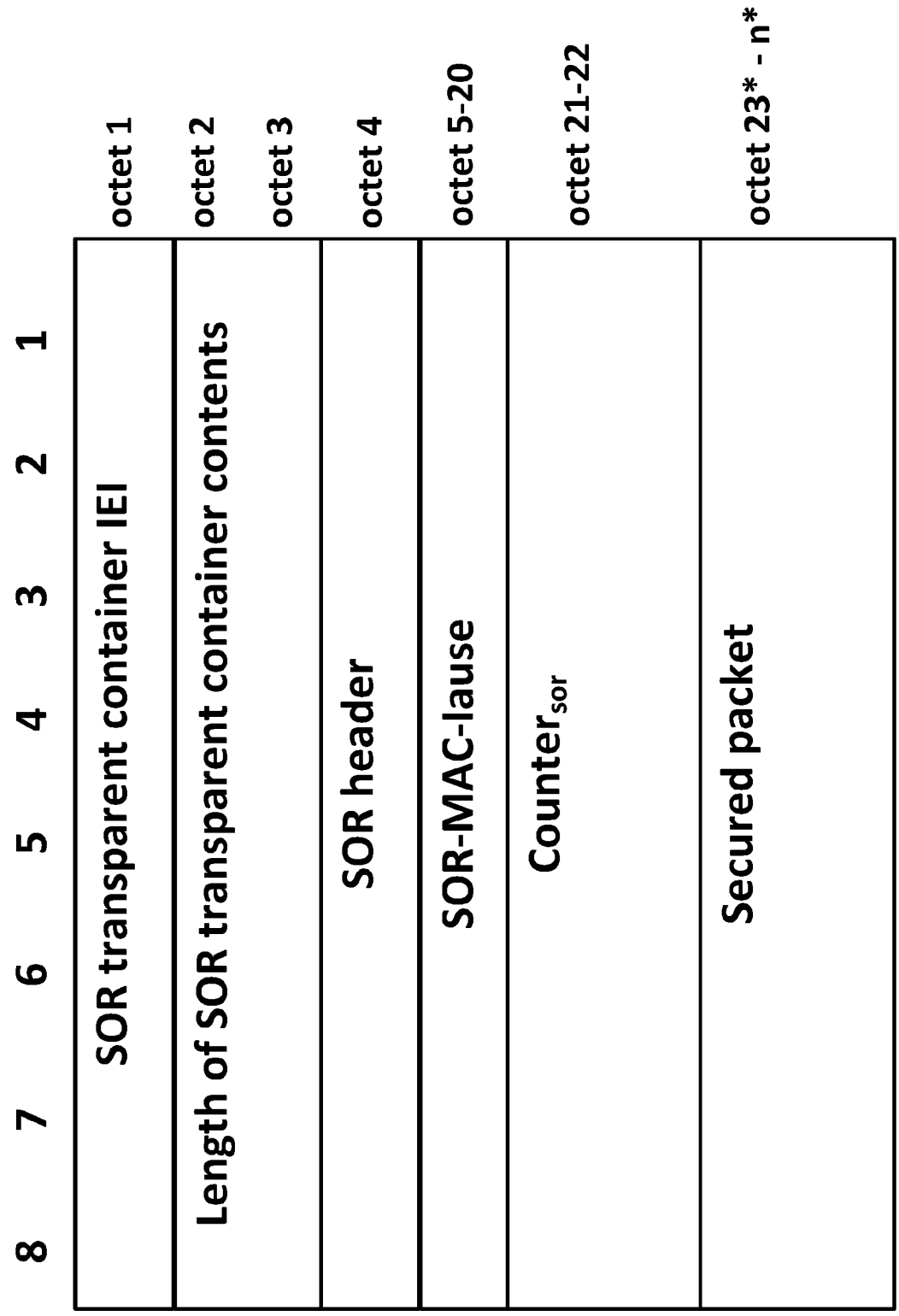
8 7 6 5 4 3 2 1
SOR transparent container IEI
Length of SOR transparent container contents
SOR header
SOR-MAC-lause
Counter$_{sor}$
Secured packet
octet 1
octet 2
octet 3
octet 4
octet 5-20
octet 21-22
octet 23* - n*

Figure 7

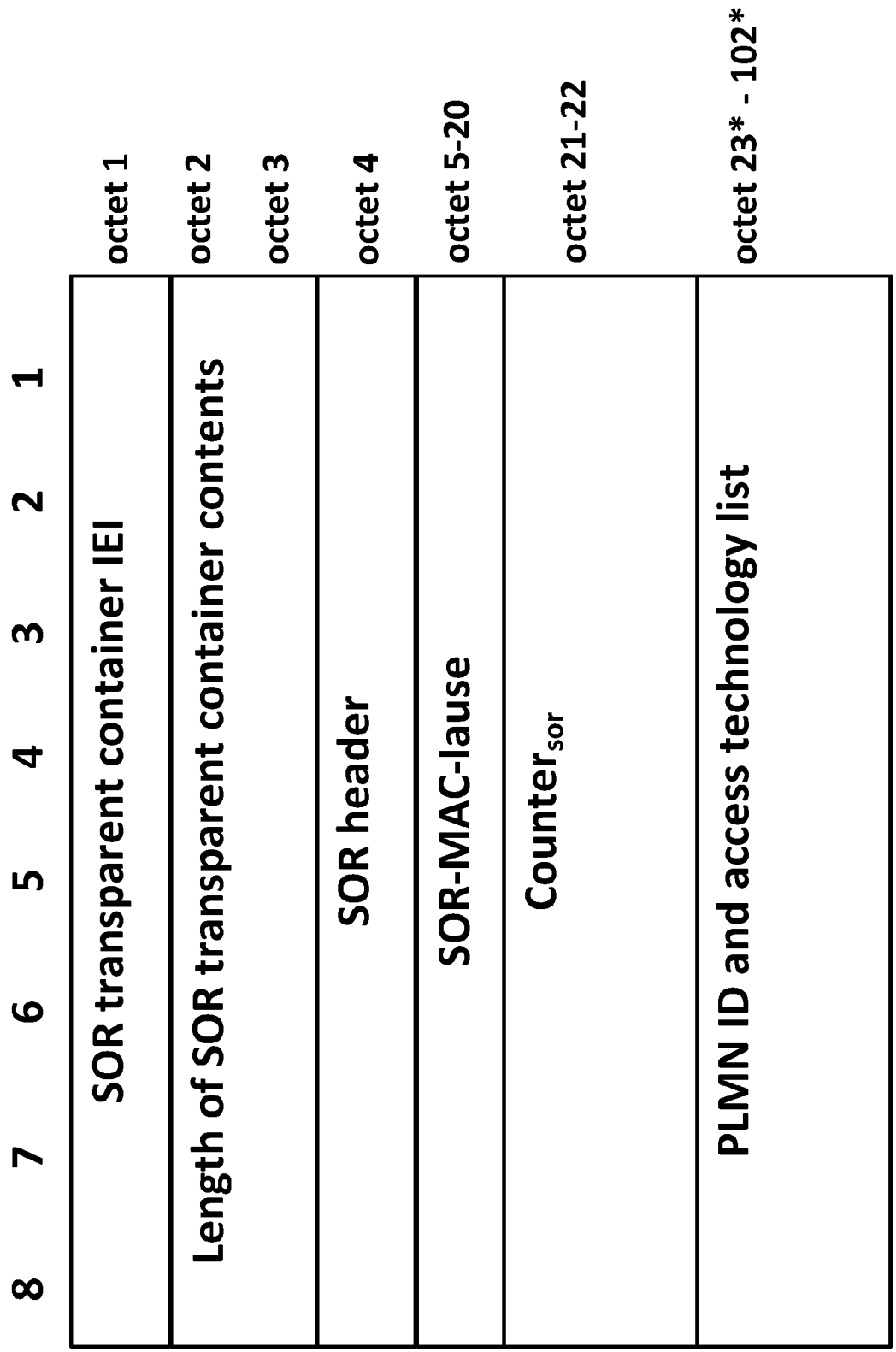
8 7 6 5 4 3 2 1
SOR transparent container IEI
Length of SOR transparent container contents
SOR header
SOR-MAC-lause
Counter$_{SOR}$
PLMN ID and access technology list
octet 1
octet 2
octet 3
octet 4
octet 5-20
octet 21-22
octet 23* - 102*

Figure 8

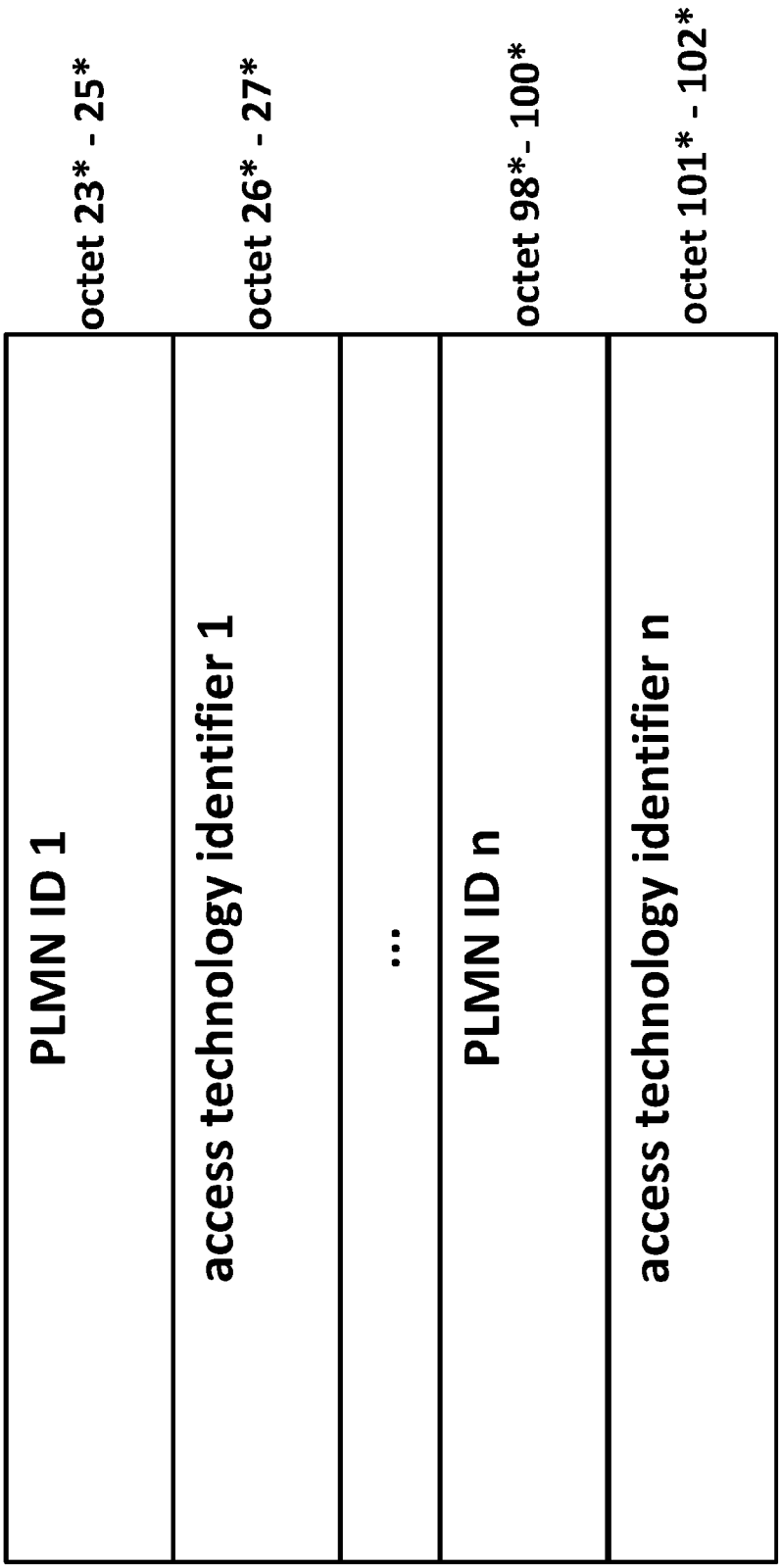
octet 23* - 25*
octet 26* - 27*
octet 98*- 100*
octet 101* - 102*
PLMN ID 1
access technology identifier 1
...
PLMN ID n
access technology identifier n

Figure 9

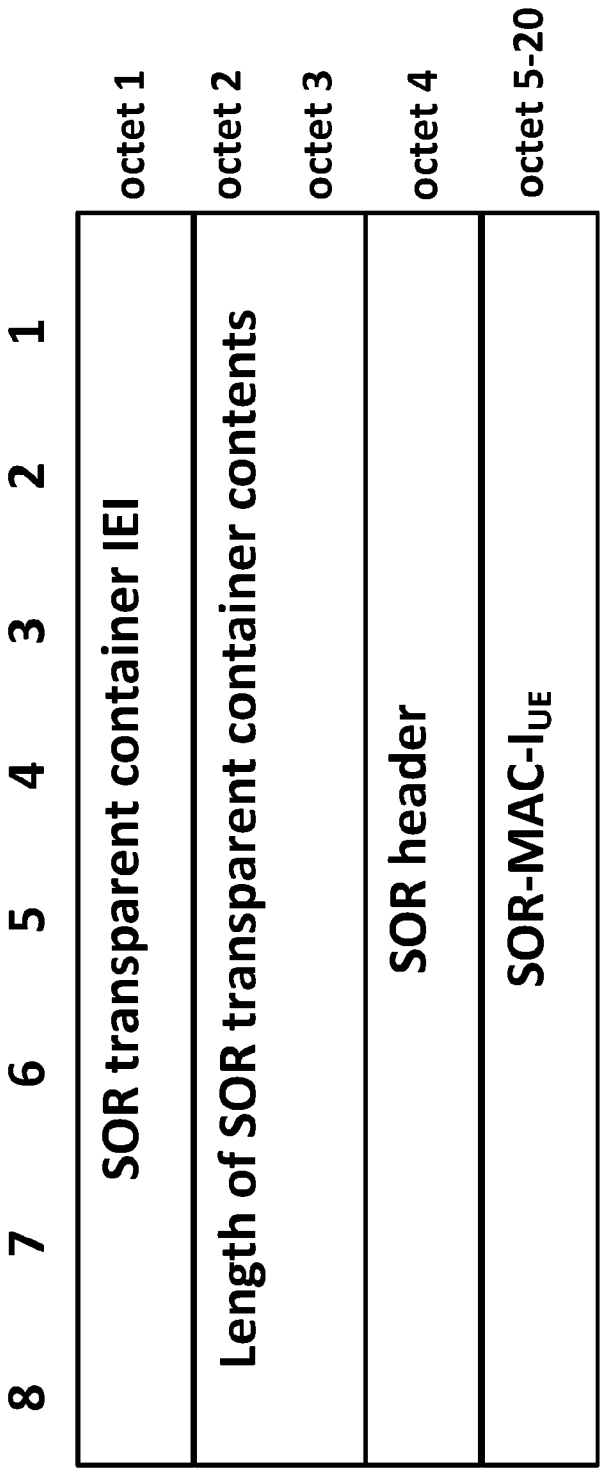
8 7 6 5 4 3 2 1
SOR transparent container IEI
Length of SOR transparent container contents
SOR header
SOR-MAC-I$_{UE}$
octet 1
octet 2
octet 3
octet 4
octet 5-20

Figure 10




Figure 11

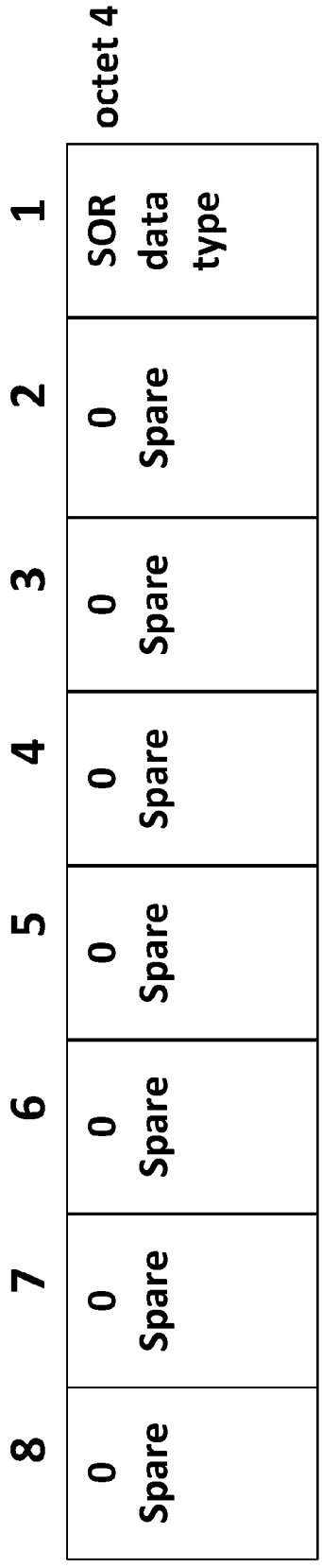


Figure 12

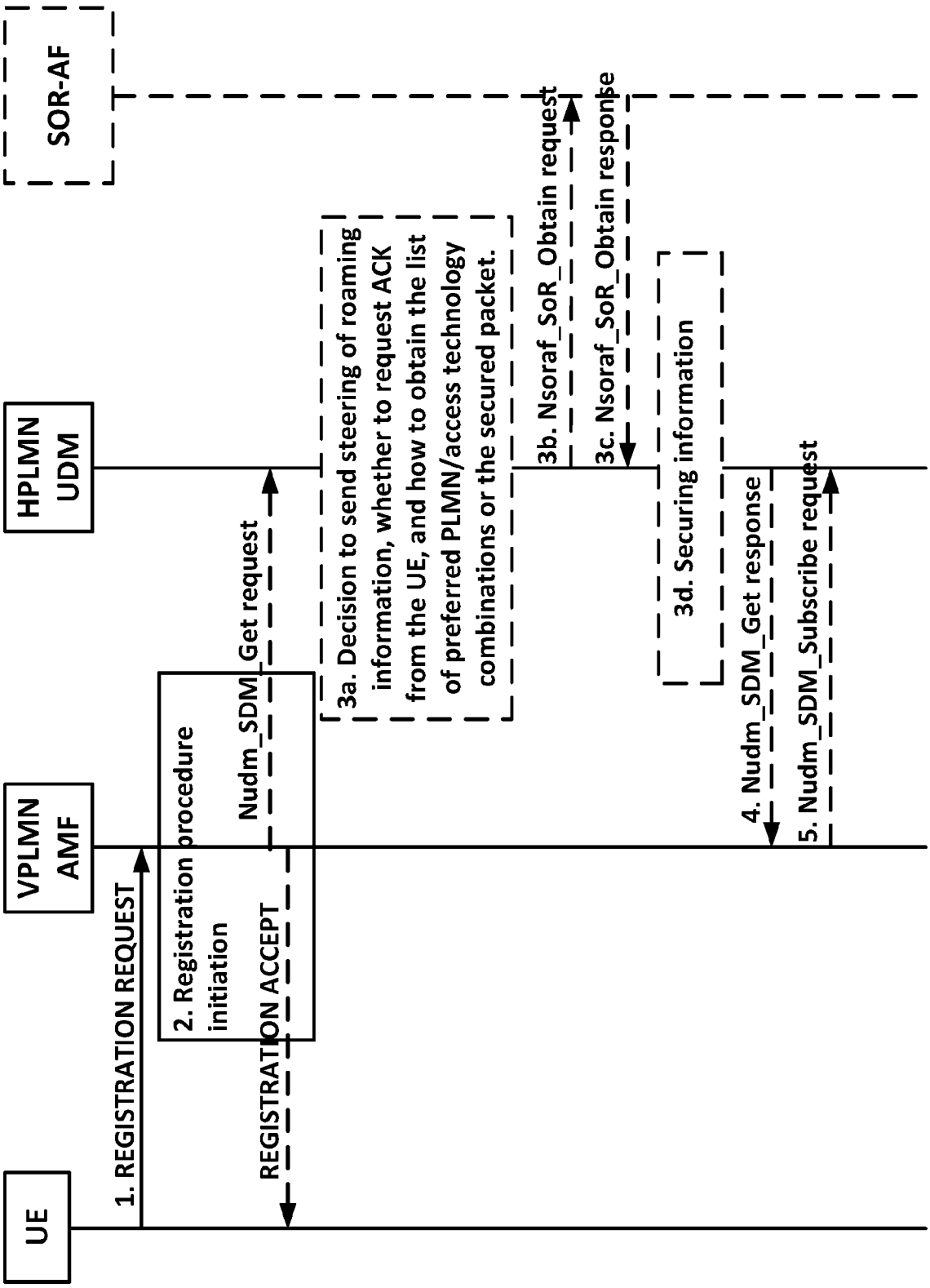
SOR-AF
HPLMN UDM
VPLMN AMF
UE
1. REGISTRATION REQUEST
2. Registration procedure initiation
Nudm_SDM_Get request
3a. Decision to send steering of roaming information, whether to request ACK from the UE, and how to obtain the list of preferred PLMN/access technology combinations or the secured packet.
3b. Nsoraf_SoR_Obtain request
3c. Nsoraf_SoR_Obtain response
3d. Securing information
4. Nudm_SDM_Get response
5. Nudm_SDM_Subscribe request
REGISTRATION ACCEPT

Figure 13A

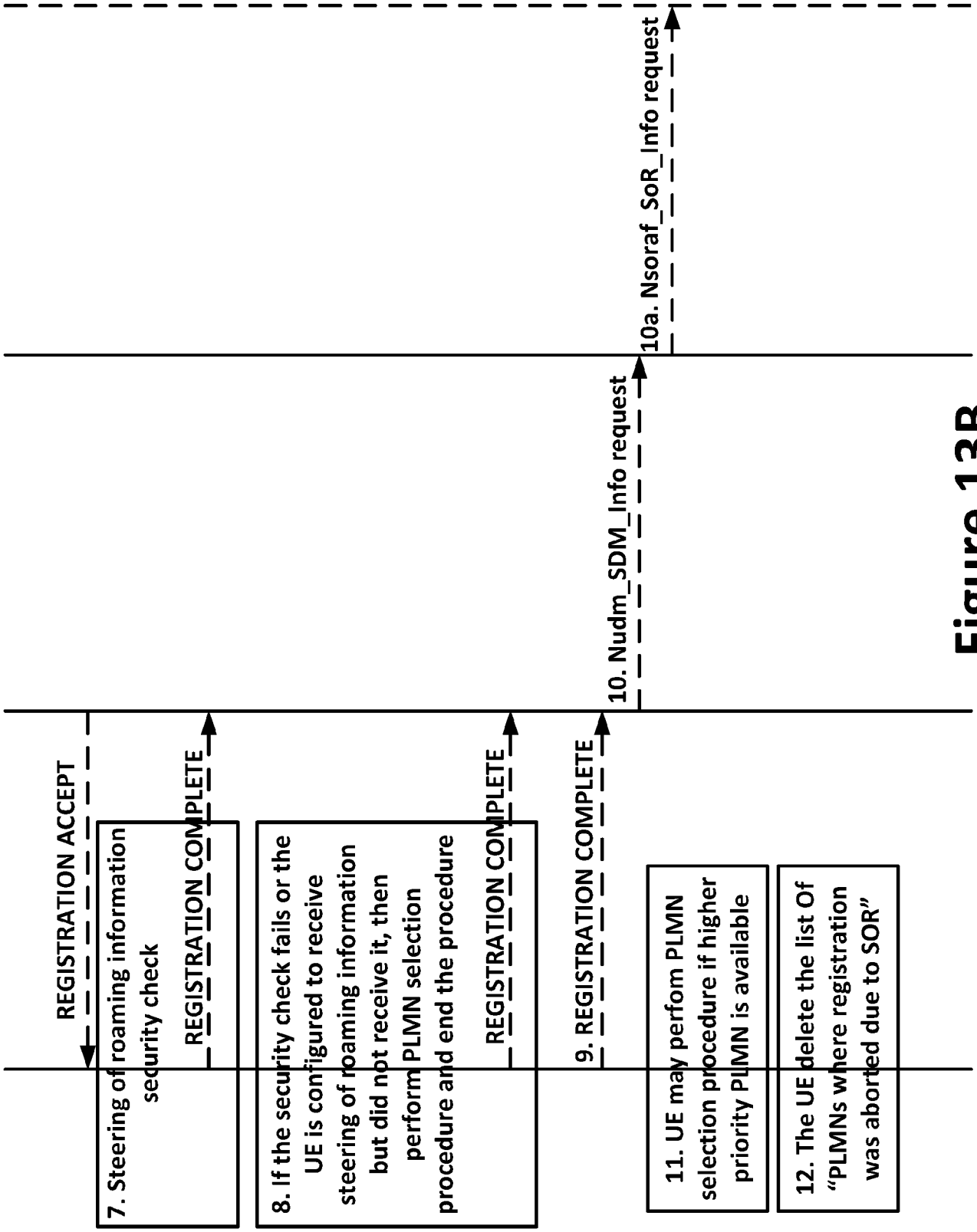
10a. Nsoraf_SoR_Info request
10. Nudm_SDM_Info request
REGISTRATION ACCEPT
7. Steering of roaming information security check
REGISTRATION COMPLETE
8. If the security check fails or the UE is configured to receive steering of roaming information but did not receive it, then perform PLMN selection procedure and end the procedure
REGISTRATION COMPLETE
9. REGISTRATION COMPLETE
11. UE may perfom PLMN selection procedure if higher priority PLMN is available
12. The UE delete the list Of "PLMNs where registration was aborted due to SOR"

Figure 13B

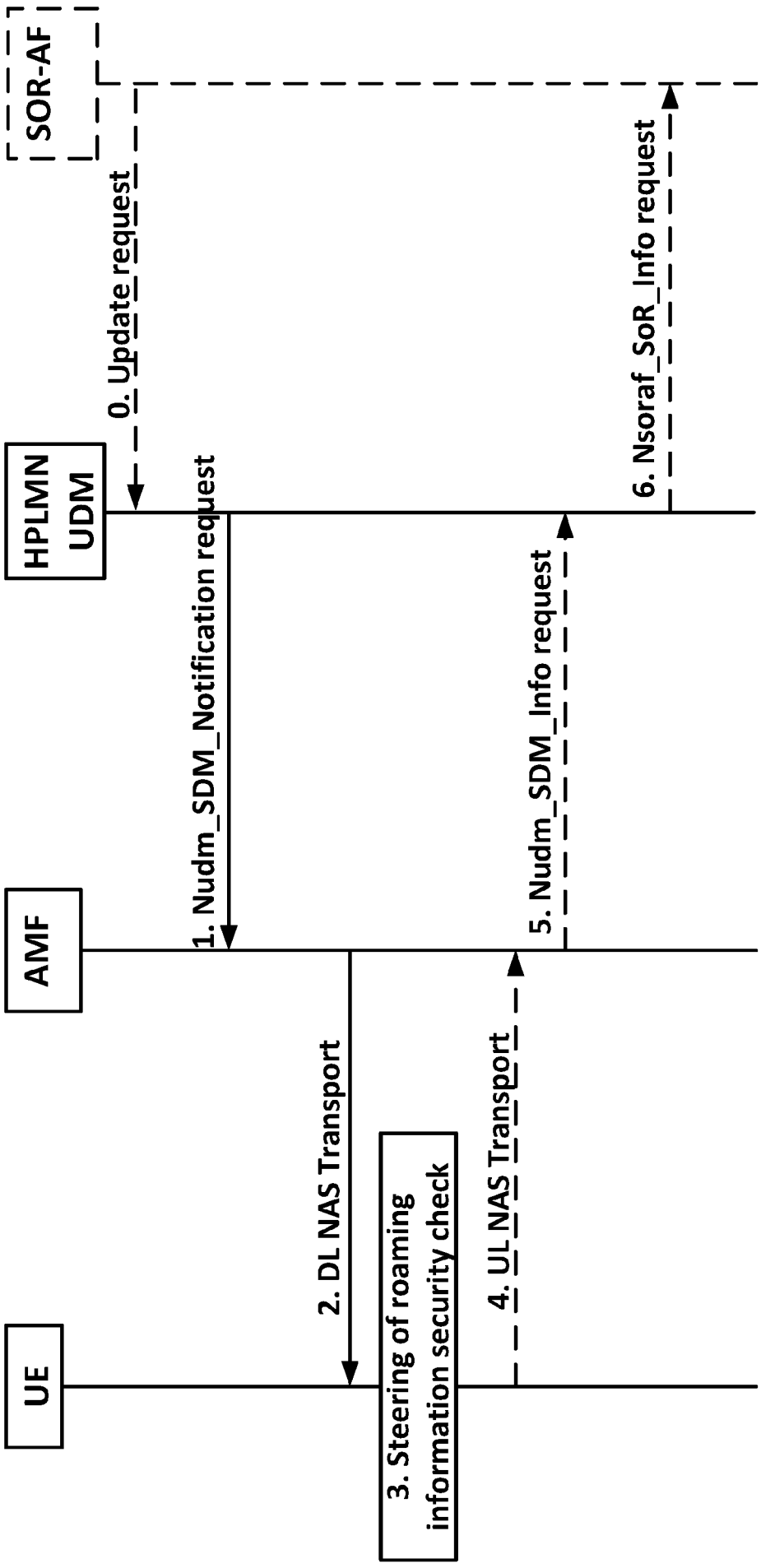
SOR-AF
HPLMN UDM
AMF
UE
0. Update request
1. Nudm_SDM_Notification request
2. DL NAS Transport
3. Steering of roaming information security check
4. UL NAS Transport
5. Nudm_SDM_Info request
6. Nsoraf_SoR_Info request

Figure 14

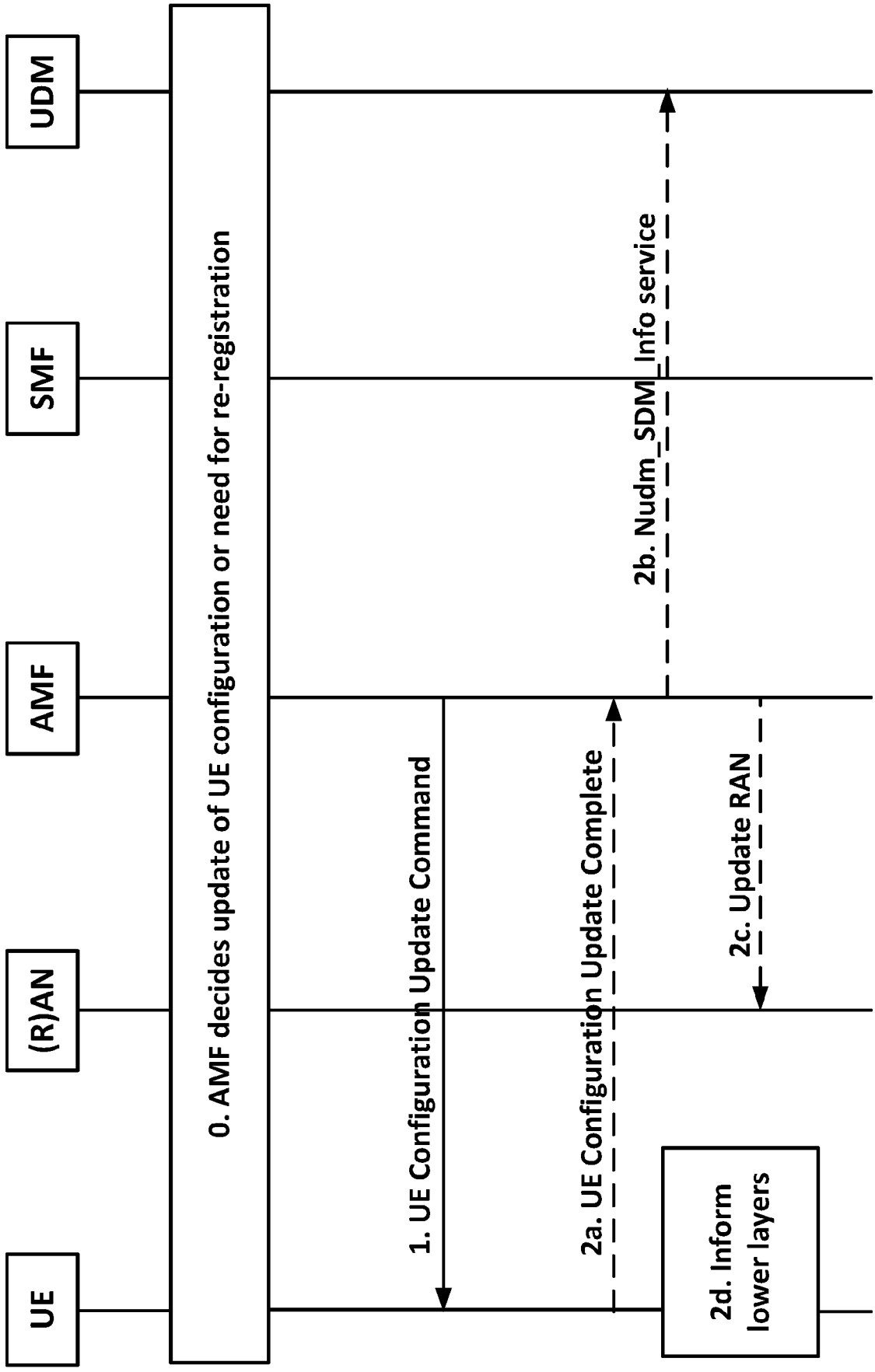
UDM
SMF
AMF
(R)AN
UE
0. AMF decides update of UE configuration or need for re-registration
2b. Nudm_SDM_Info service
1. UE Configuration Update Command
2a. UE Configuration Update Complete
2c. Update RAN
2d. Inform lower layers

Figure 15A

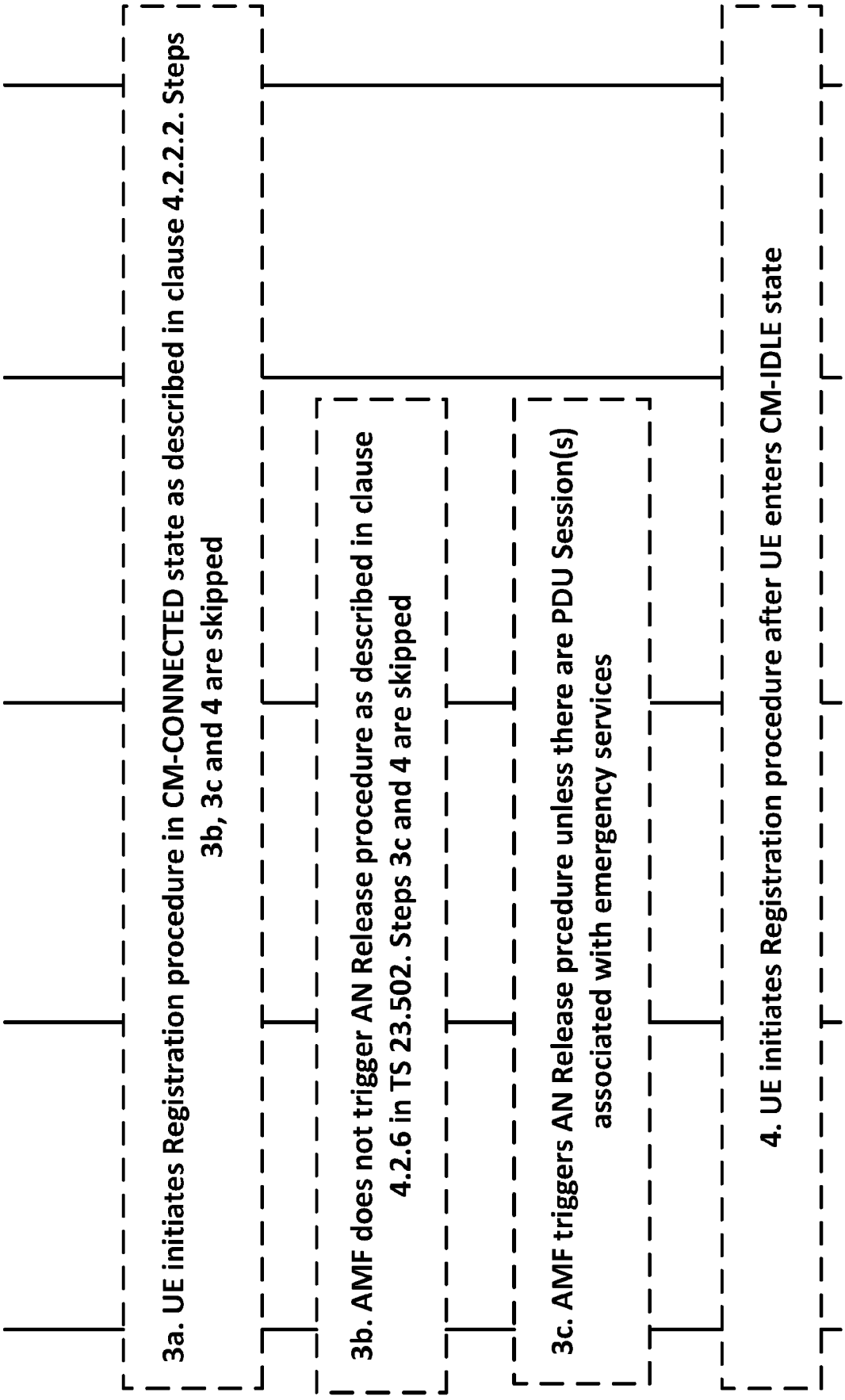
3a. UE initiates Registration procedure in CM-CONNECTED state as described in clause 4.2.2.2. Steps 3b, 3c and 4 are skipped
3b. AMF does not trigger AN Release procedure as described in clause 4.2.6 in TS 23.502. Steps 3c and 4 are skipped
3c. AMF triggers AN Release prcedure unless there are PDU Session(s) associated with emergency services
4. UE initiates Registration procedure after UE enters CM-IDLE state

Figure 15B

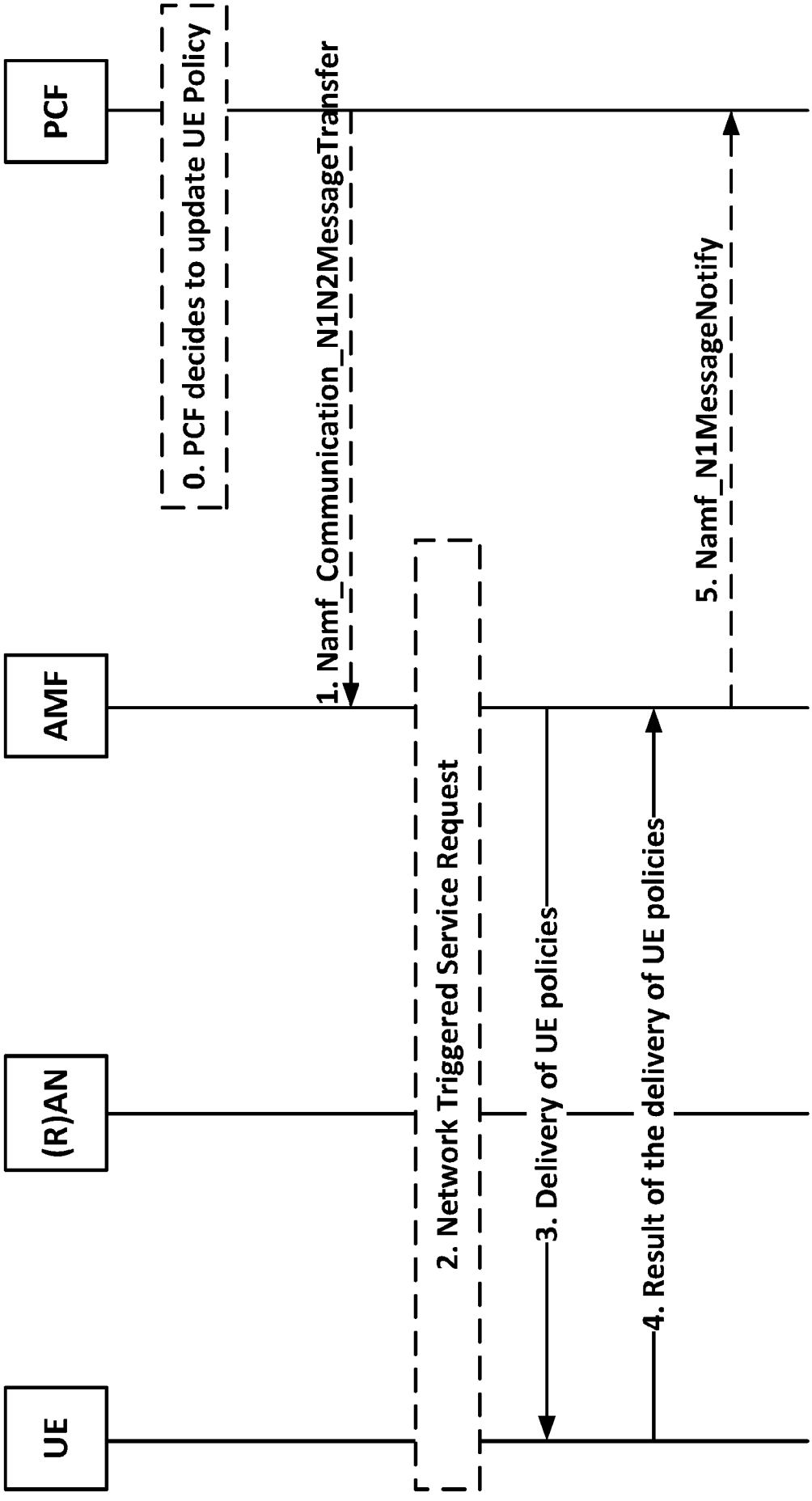
PCF
AMF
(R)AN
UE
0. PCF decides to update UE Policy
1. Namf_Communication_N1N2MessageTransfer
2. Network Triggered Service Request
3. Delivery of UE policies
4. Result of the delivery of UE policies
5. Namf_N1MessageNotify

Figure 16

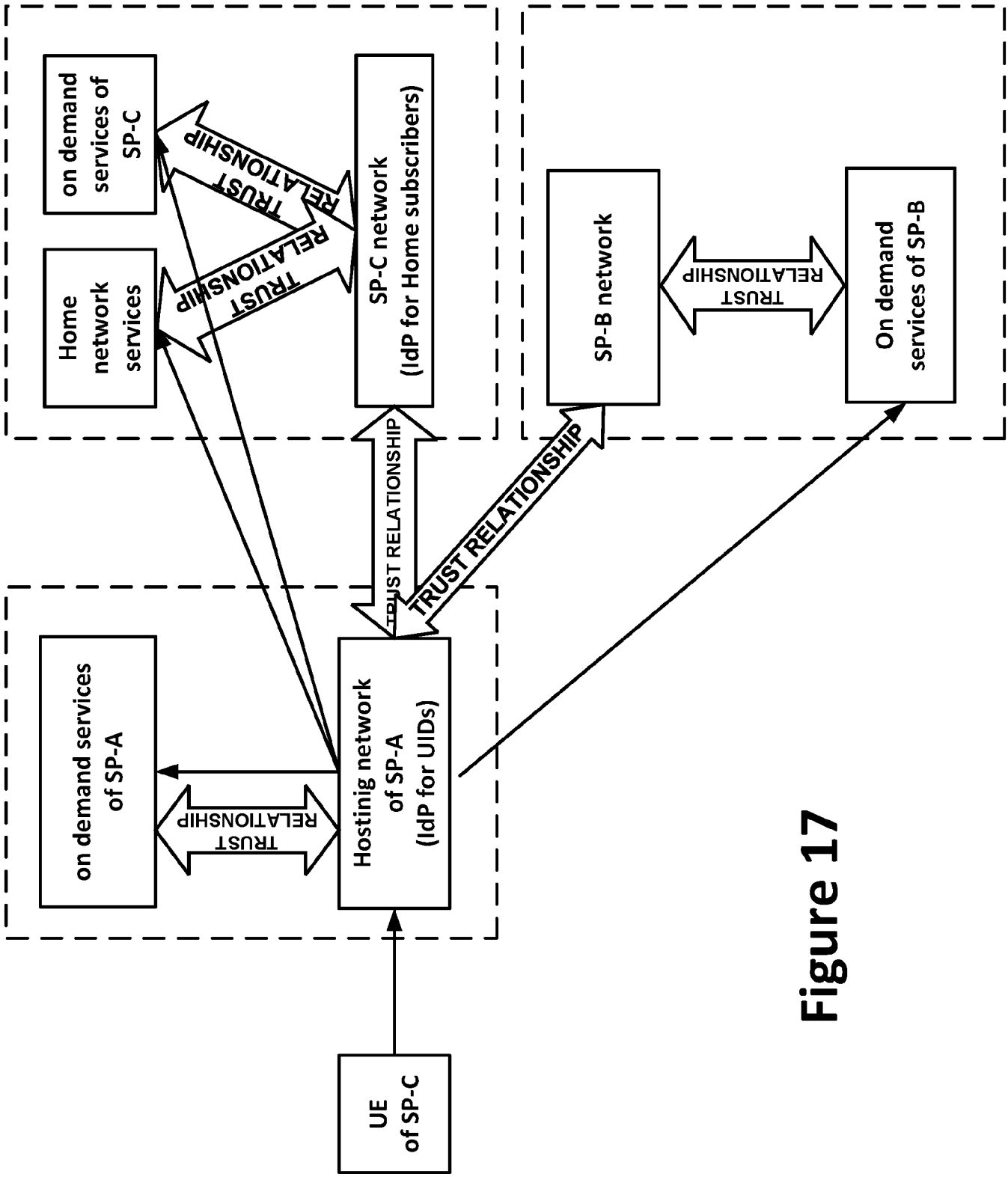
on demand services of SP-C
Home network services
SP-C network (IdP for Home subscribers)
TRUST RELATIONSHIP
TRUST RELATIONSHIP
SP-B network
TRUST RELATIONSHIP
On demand services of SP-B
TRUST RELATIONSHIP
TRUST RELATIONSHIP
on demand services of SP-A
Hostinig network of SP-A (IdP for UIDs)
UE of SP-C

Figure 17

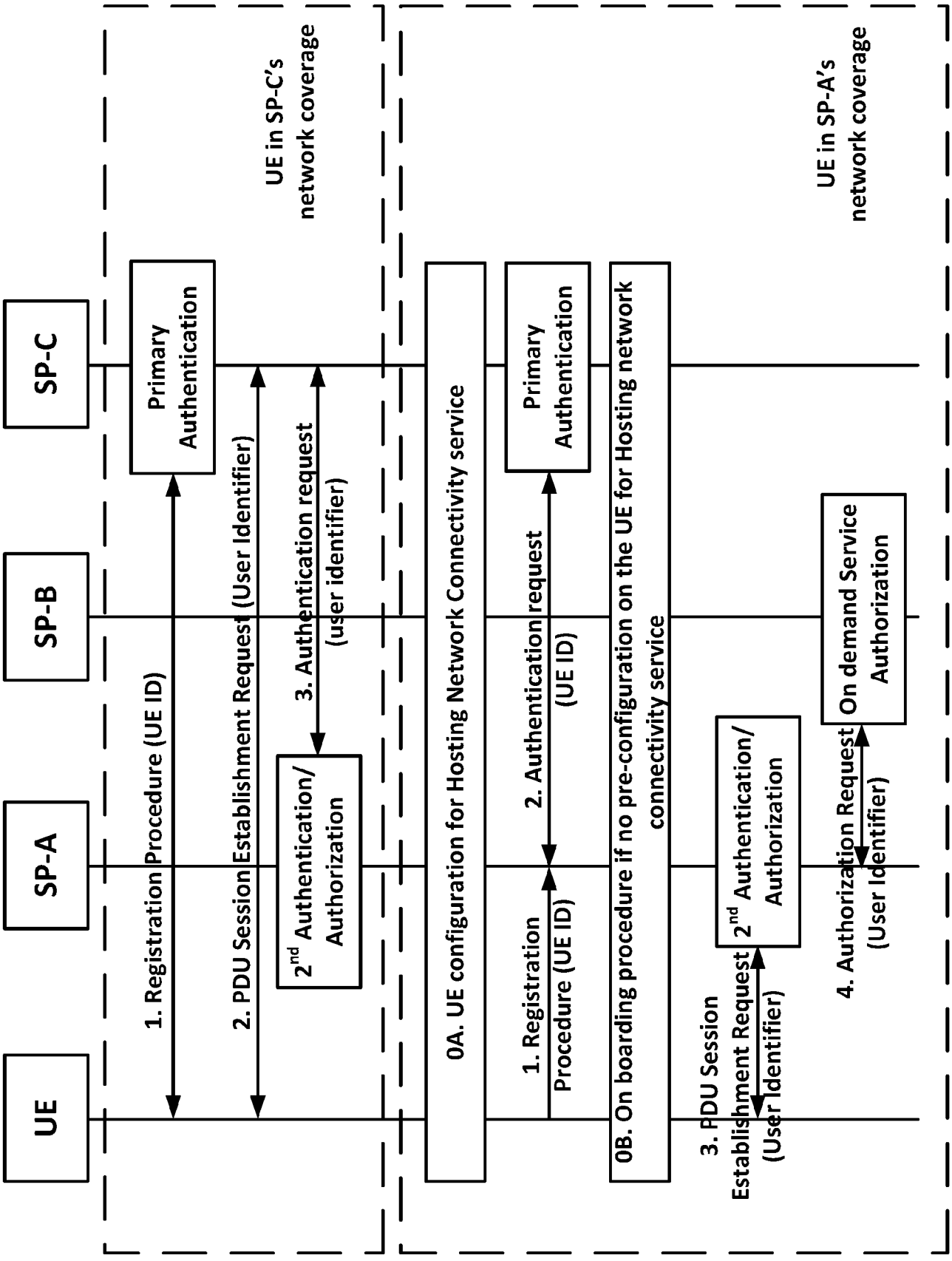
UE
SP-A
SP-B
SP-C
UE in SP-C's network coverage
UE in SP-A's network coverage
1. Registration Procedure (UE ID)
Primary Authentication
2. PDU Session Establishment Request (User Identifier)
3. Authentication request (user identifier)
2nd Authentication/ Authorization
0A. UE configuration for Hosting Network Connectivity service
1. Registration Procedure (UE ID)
2. Authentication request (UE ID)
Primary Authentication
0B. On boarding procedure if no pre-configuration on the UE for Hosting network connectivity service
3. PDU Session Establishment Request (User Identifier)
2nd Authentication/ Authorization
4. Authorization Request (User Identifier)
On demand Service Authorization

Figure 18

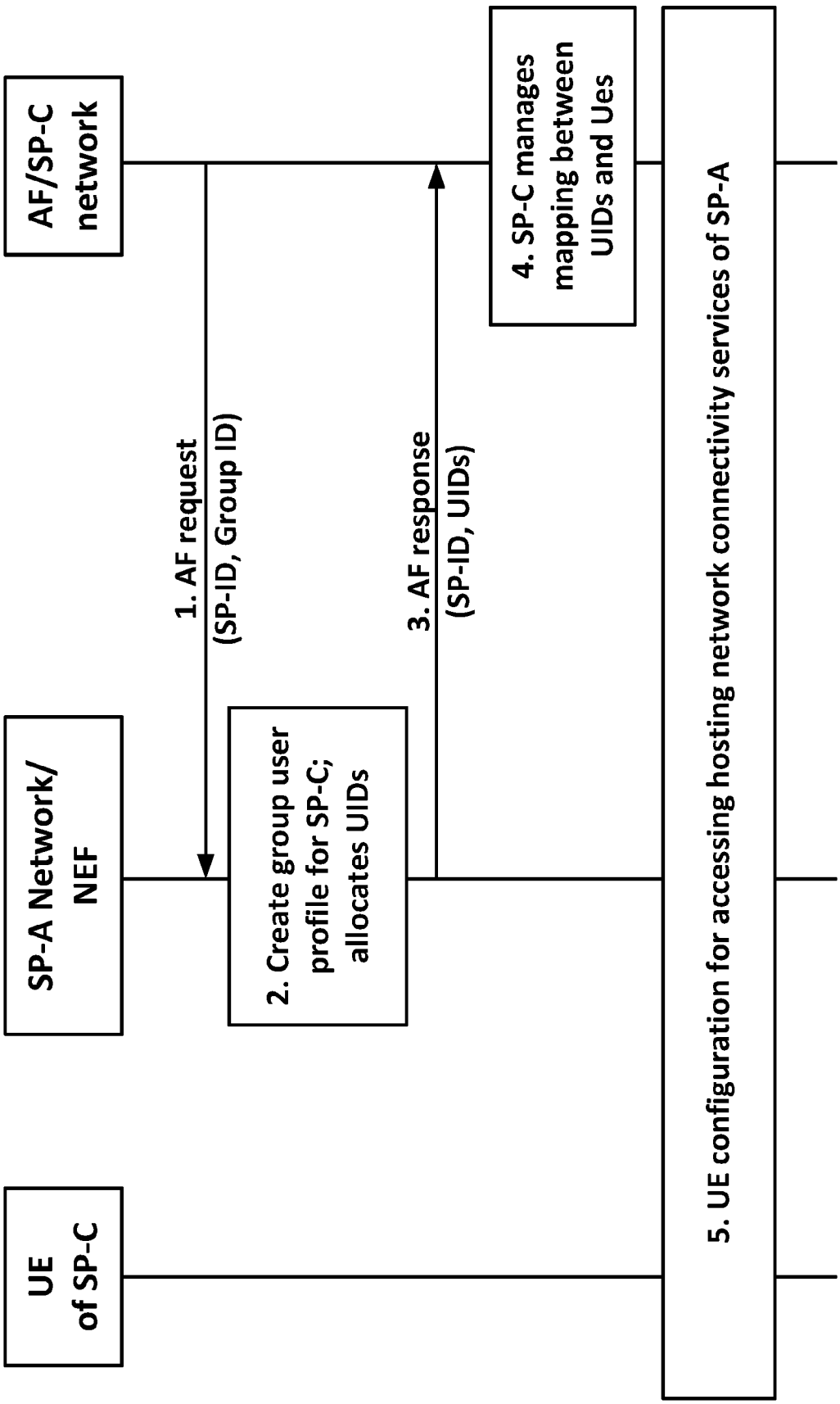
AF/SP-C network
SP-A Network/ NEF
UE of SP-C
1. AF request (SP-ID, Group ID)
2. Create group user profile for SP-C; allocates UIDs
3. AF response (SP-ID, UIDs)
4. SP-C manages mapping between UIDs and Ues
5. UE configuration for accessing hosting network connectivity services of SP-A

Figure 19

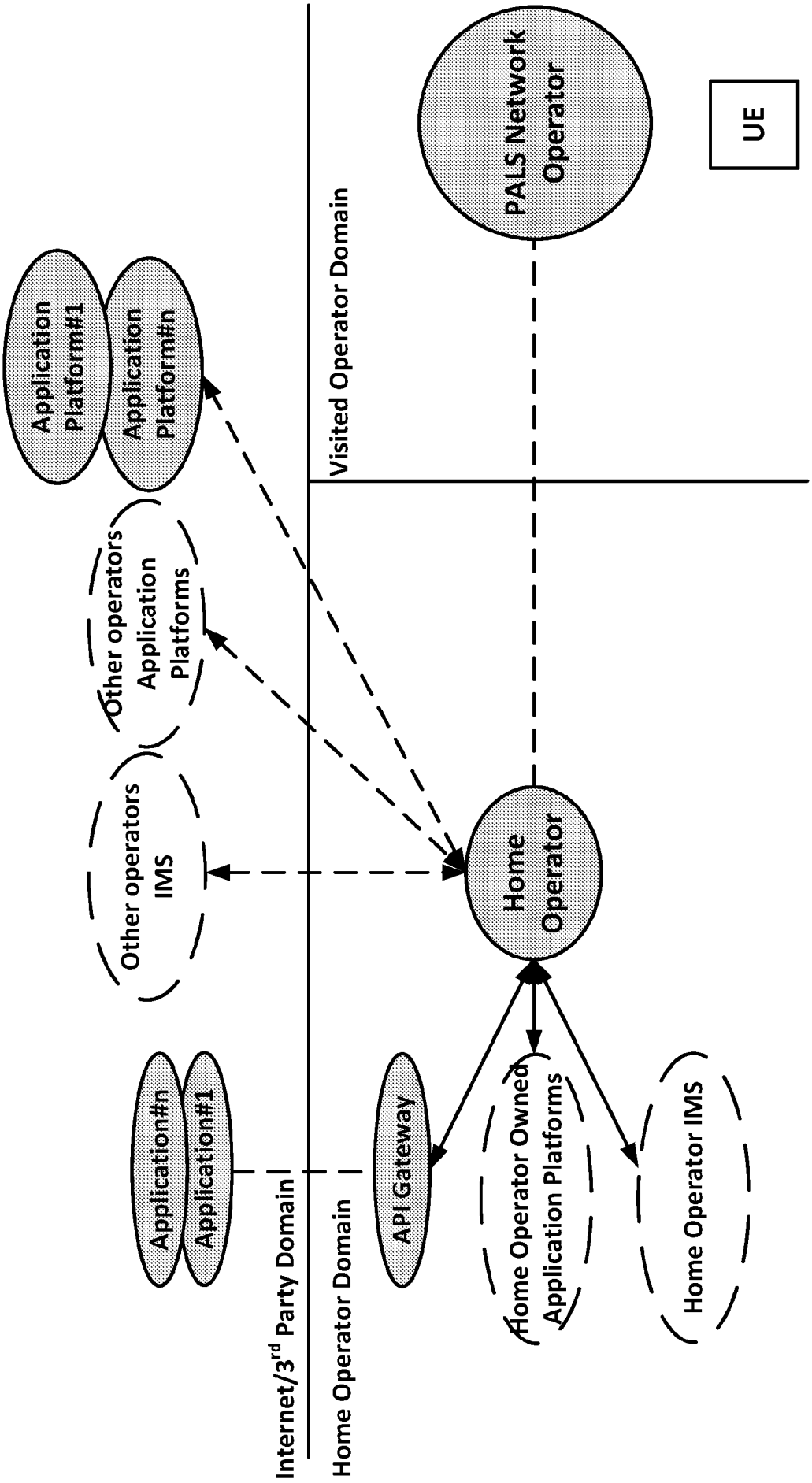
Application Platform#1
Application Platform#n
Other operators Application Platforms
Other operators IMS
Application#n
Application#1
API Gateway
Home Operator Owned Application Platforms
Home Operator IMS
Internet/3rd Party Domain
Home Operator Domain
Visited Operator Domain
PALS Network Operator
UE
Home Operator

Figure 20

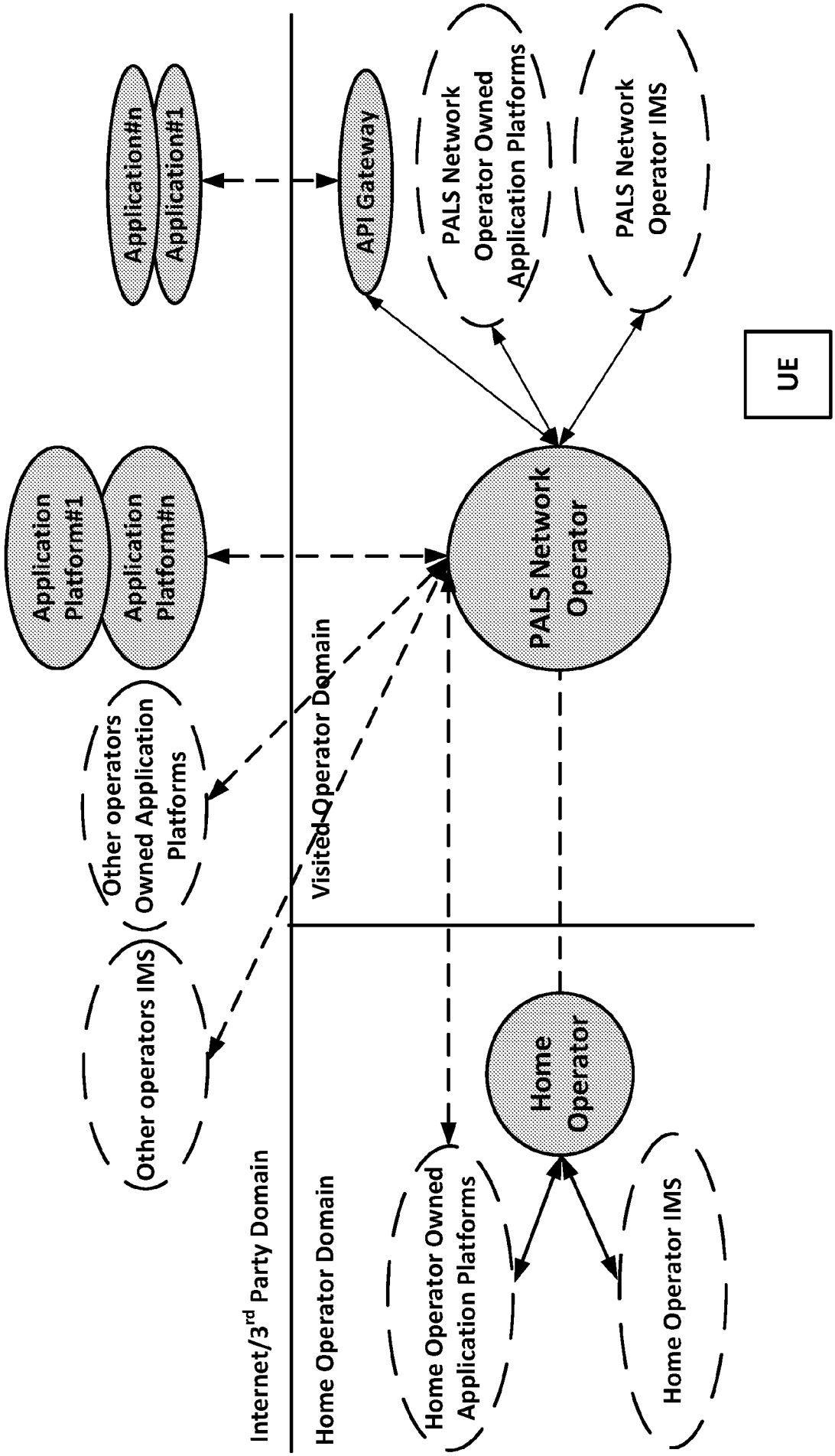
Application#n
Application#1
API Gateway
PALS Network Operator Owned Application Platforms
PALS Network Operator IMS
UE
Application Platform#1
Application Platform#n
PALS Network Operator
Other operators Owned Application Platforms
Other operators IMS
Visited Operator Domain
Home Operator
Home Operator Owned Application Platforms
Home Operator IMS
Home Operator Domain
Internet/3rd Party Domain

Figure 21

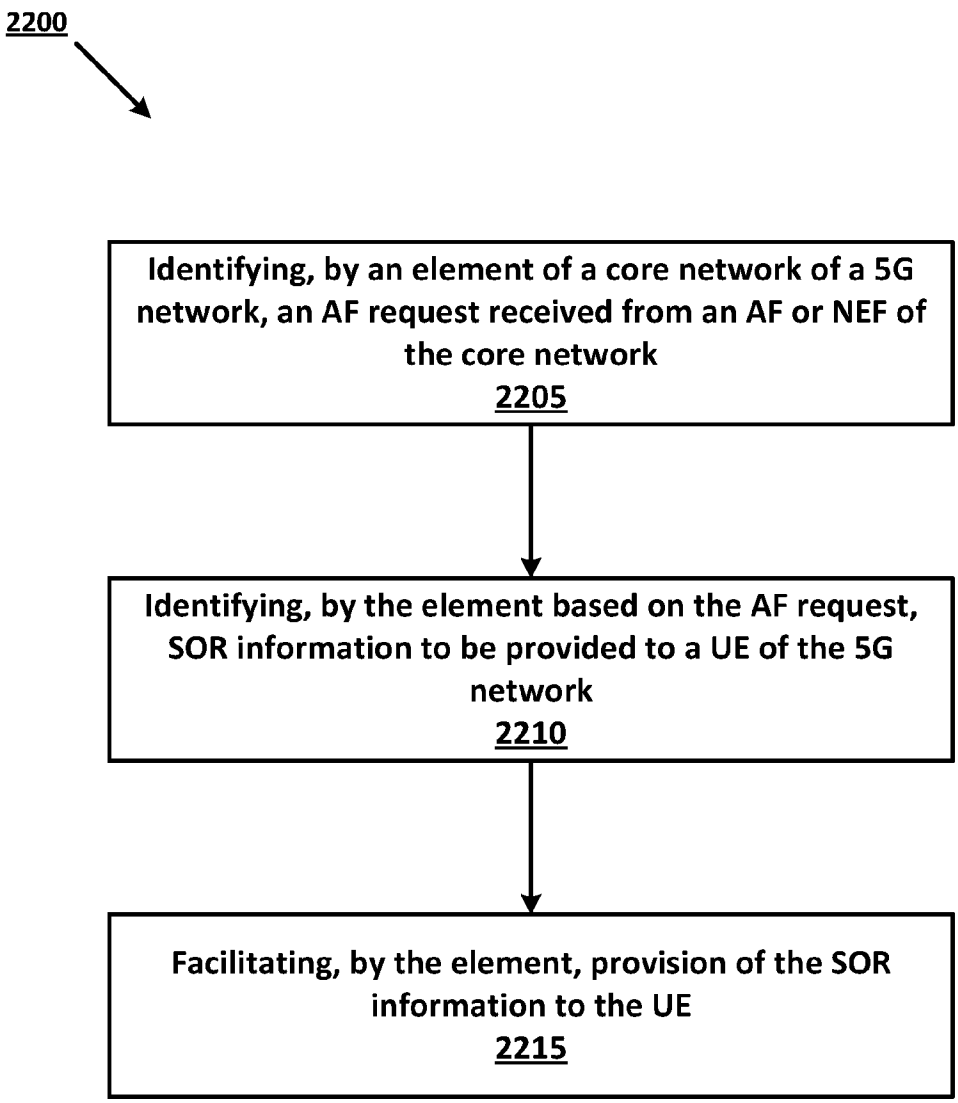
2200
Identifying, by an element of a core network of a 5G network, an AF request received from an AF or NEF of the core network
2205
Identifying, by the element based on the AF request, SOR information to be provided to a UE of the 5G network
2210
Facilitating, by the element, provision of the SOR information to the UE
2215

Figure 22

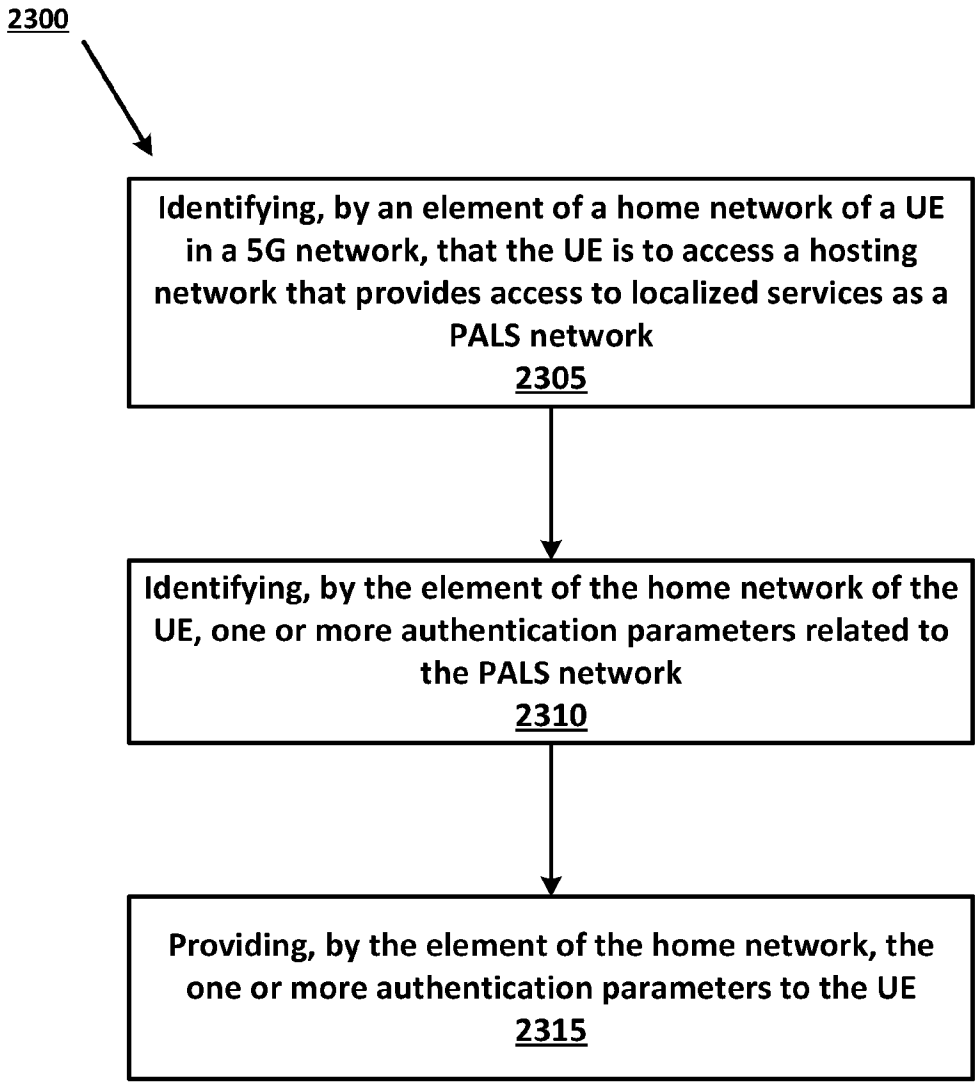
2300
Identifying, by an element of a home network of a UE in a 5G network, that the UE is to access a hosting network that provides access to localized services as a PALS network
2305
Identifying, by the element of the home network of the UE, one or more authentication parameters related to the PALS network
2310
Providing, by the element of the home network, the one or more authentication parameters to the UE
2315

Figure 23

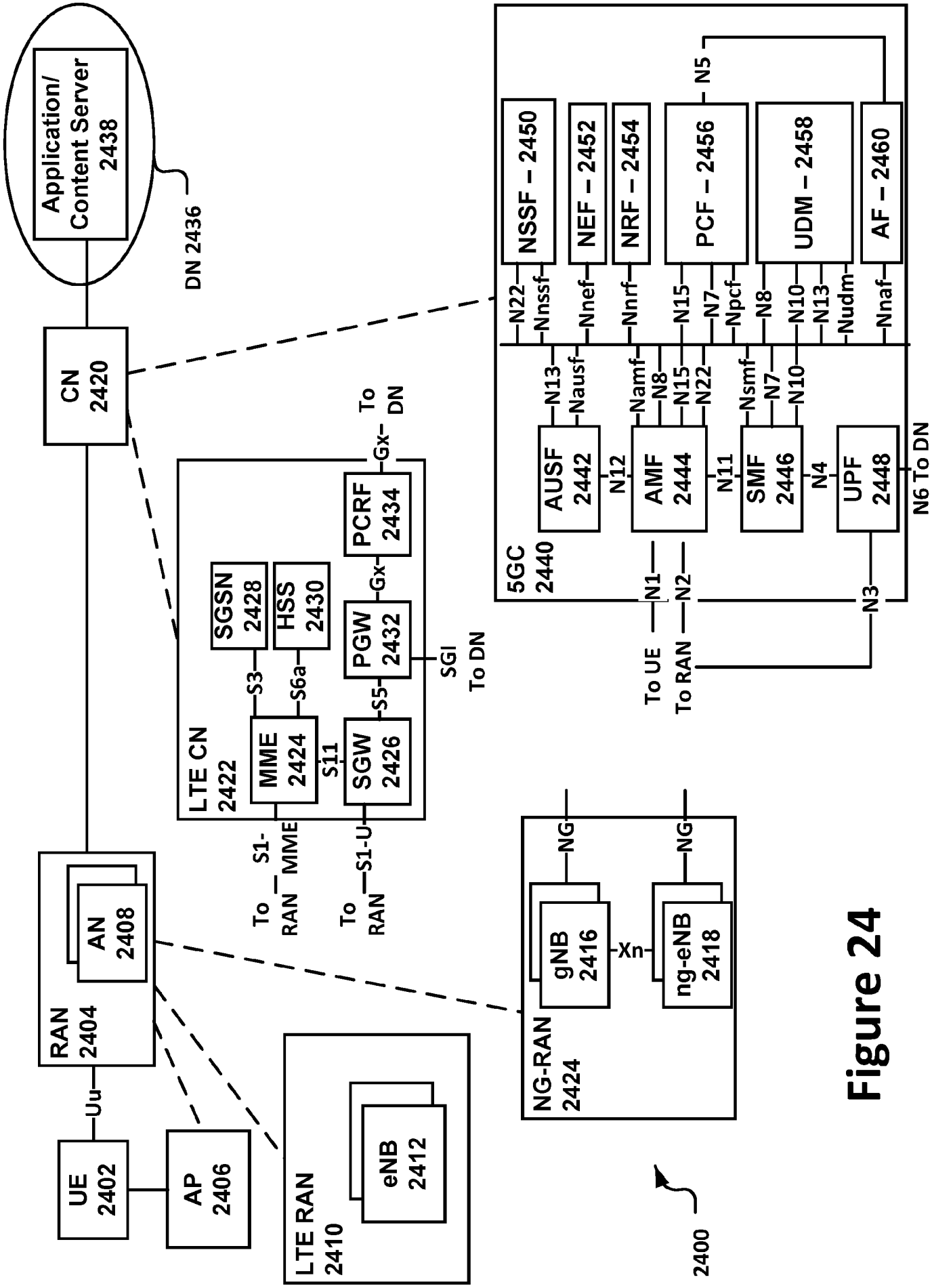
Application/ Content Server 2438
DN 2436
CN 2420
RAN 2404
AN 2408
UE 2402
Uu
AP 2406
LTE RAN 2410
eNB 2412
LTE CN 2422
MME 2424
SGW 2426
PGW 2432
PCRF 2434
SGSN 2428
HSS 2430
S3
S6a
S11
S5
Gx
SGI
To DN
To RAN
S1-MME
S1-U
NG-RAN 2424
gNB 2416
ng-eNB 2418
Xn
NG
5GC 2440
AUSF 2442
AMF 2444
SMF 2446
UPF 2448
N1
N2
N3
N4
N5
N6 To DN
N7
N8
N10
N11
N12
N13
N15
N22
Nausf
Namf
Nsmf
Nnssf
Nnef
Nnrf
Npcf
Nudm
Nnaf
NSSF – 2450
NEF – 2452
NRF – 2454
PCF – 2456
UDM – 2458
AF – 2460
To UE
To RAN
2400

Figure 24

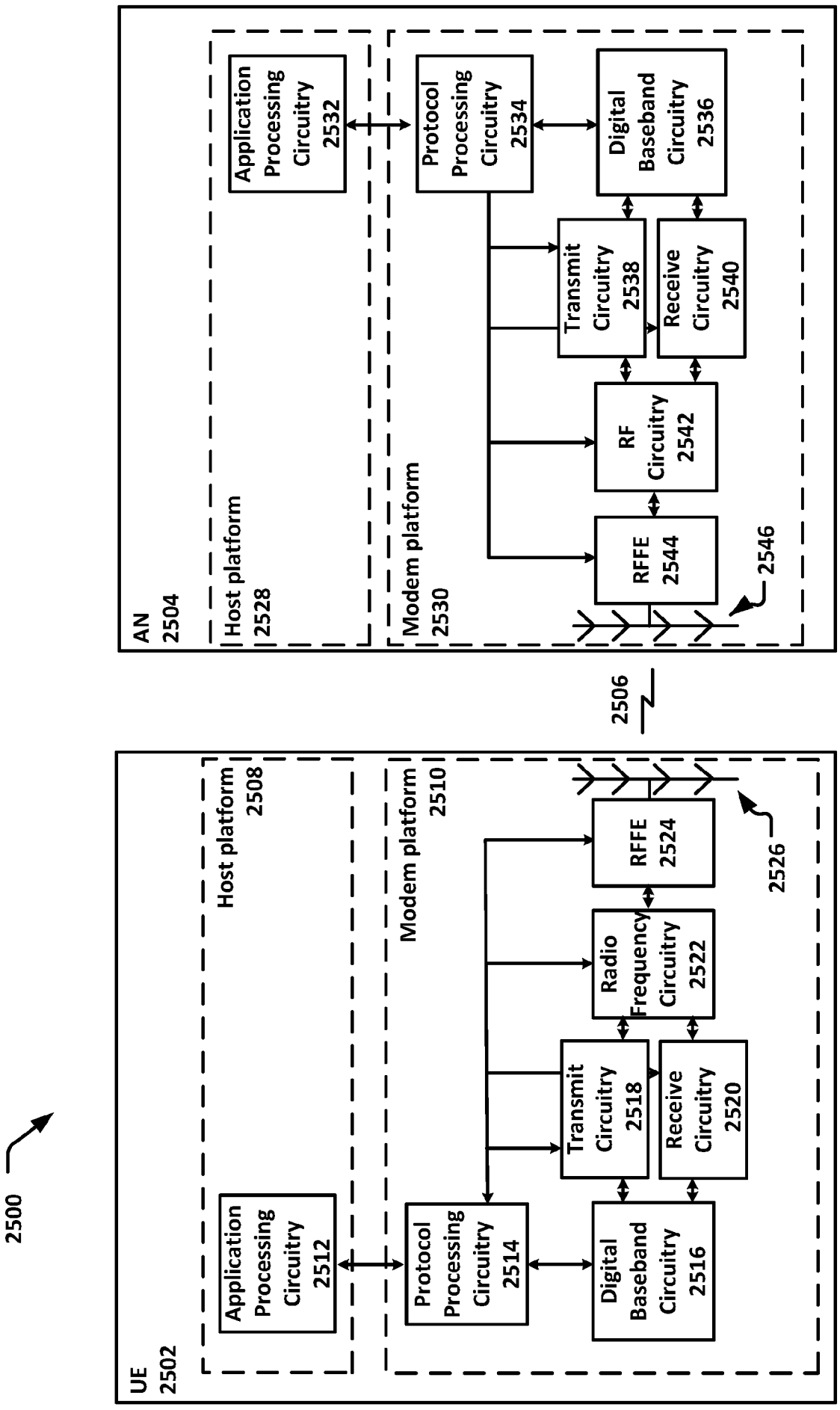
2500
UE
2502
Application Processing Circuitry 2512
Host platform 2508
Protocol Processing Circuitry 2514
Digital Baseband Circuitry 2516
Transmit Circuitry 2518
Receive Circuitry 2520
Radio Frequency Circuitry 2522
RFFE 2524
Modem platform 2510
2526
2506
AN
2504
Application Processing Circuitry 2532
Host platform 2528
Protocol Processing Circuitry 2534
Digital Baseband Circuitry 2536
Transmit Circuitry 2538
Receive Circuitry 2540
RF Circuitry 2542
RFFE 2544
Modem platform 2530
2546

Figure 25

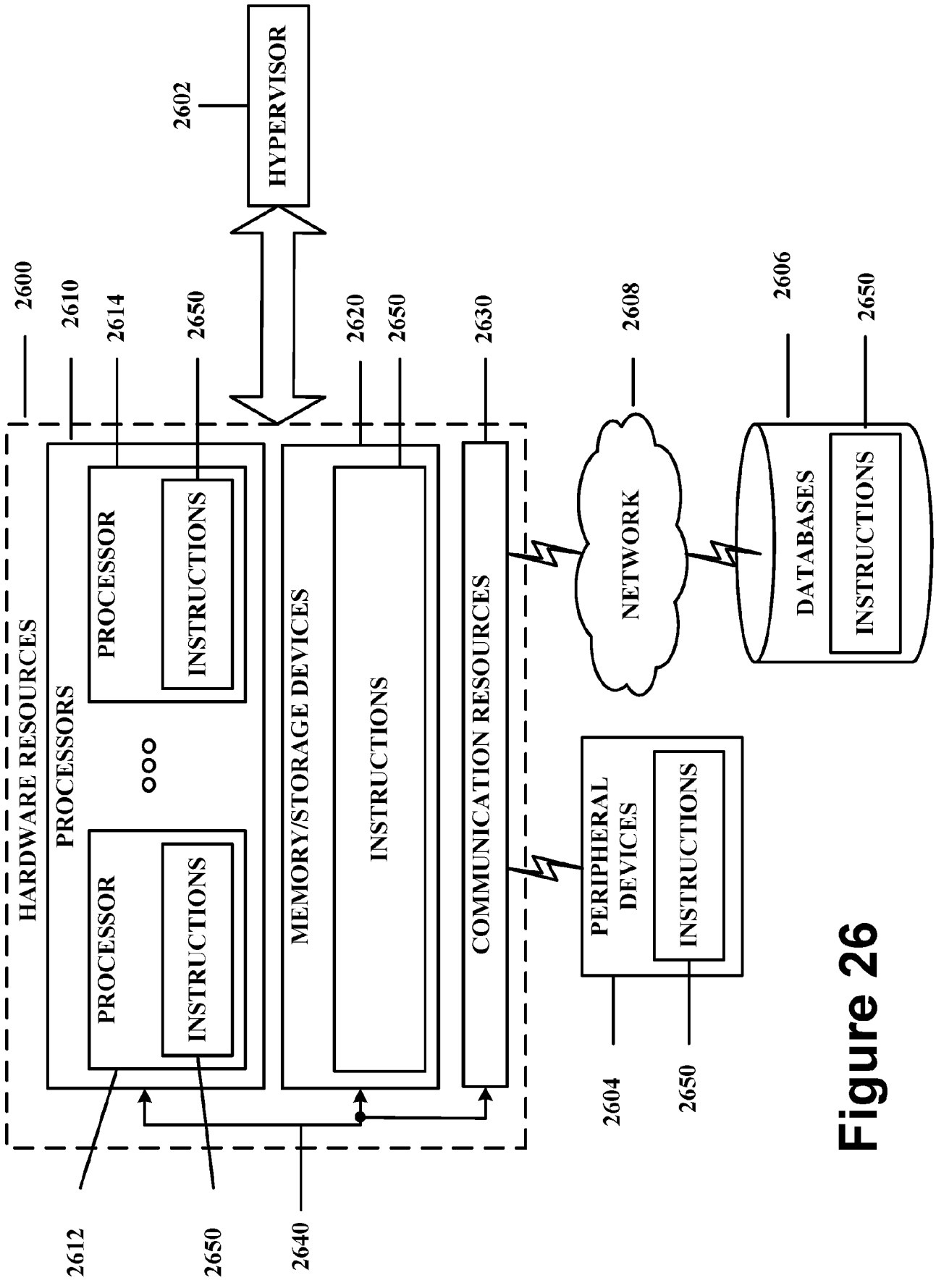
HYPERVISOR
2602
HARDWARE RESOURCES
2600
PROCESSORS
2610
PROCESSOR
2614
INSTRUCTIONS
2650
PROCESSOR
INSTRUCTIONS
MEMORY/STORAGE DEVICES
2620
INSTRUCTIONS
2650
COMMUNICATION RESOURCES
2630
NETWORK
2608
DATABASES
2606
INSTRUCTIONS
2650
PERIPHERAL DEVICES
2604
INSTRUCTIONS
2650
2612
2650
2640

Figure 26

# INTERNATIONAL SEARCH REPORT

International application No.
**PCT/US2022/014430**

## A. CLASSIFICATION OF SUBJECT MATTER

**H04W 8/08**(2009.01)i; **H04W 4/50**(2018.01)i; **H04W 12/069**(2021.01)i; **H04W 12/72**(2021.01)i; **H04W 84/10**(2009.01)i; **H04W 84/04**(2009.01)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 8/08(2009.01); H04L 29/06(2006.01); H04W 8/04(2009.01); H04W 8/16(2009.01)

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Korean utility models and applications for utility models
Japanese utility models and applications for utility models

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS(KIPO internal) & Keywords: AF request, steering of roaming (SOR), HPLMN, VPLMN, UDM, UDR, AMF, validity, PALS, home network, authentication

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| DY | '3GPP; TSG CT; NAS functions related to MS in idle mode (Release 17)', 3GPP TS 23.122 V17.1.1, 5 January 2021<br>pages 69-72; and figure C.2.1 | 1-10 |
| DY | '3GPP; TSG SA; Procedures for the 5GS; Stage 2 (Release 16)', 3GPP TS 23.502 V16.7.1, 13 January 2021<br>section 4.15.6.7 | 1-10,16-20 |
| DX<br>DY | '3GPP; TSG SA; Study on 5G Networks Providing Access to Localized Services; Stage 1 (Release 18)', 3 GPP TR 22.844 V0.1.0, 24 November 2020<br>sections 5.3.1-5.8.5; and figure 1 | 11-15<br>7-8,10,16-20 |
| A | US 2019-0182655 A1 (VIVEK G, GUPTA et al.) 13 June 2019 (2019-06-13)<br>paragraphs [0035]-[0061] | 1-10 |
| A | WO 2009-016967 A1 (NEC CORPORATION) 05 February 2009 (2009-02-05)<br>page 9, line 10 – page 11, line 20 | 11-20 |

☐ 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 |
|---|---|
| **04 May 2022** | **04 May 2022** |

| Name and mailing address of the ISA/KR | Authorized officer |
|---|---|
| **Korean Intellectual Property Office**<br>**189 Cheongsa-ro, Seo-gu, Daejeon**<br>**35208, Republic of Korea** | **YANG, Jeong Rok** |
| Facsimile No. **+82-42-481-8578** | Telephone No. **+82-42-481-5709** |

# INTERNATIONAL SEARCH REPORT

International application No.
**PCT/US2022/014430**

**Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)**

This International Searching Authority found multiple inventions in this international application, as follows:

Group I: Claims 1-10 directed to a method comprising: identifying, by an element of a core network of a 5G network, an AF request received from an AF or NEF of the core network; identifying steering of roaming (SOR) information to be provided to a UE of the 5G network; and facilitating provision of the SOR information to the UE.

Group II: Claims 11-20 directed to a method comrising: identifying, by an element of a home network of a UE in a 5G network, that the UE is to access to hosting network that provides access to localized services as a PALS network; identifying one or more authentication parameters related to the PALS network; and providing the one or more authentication parameters to the UE.

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☑ As all searchable claims could be searched without effort justifying additional fees, this Authority did not invite payment of additional fees.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

**Remark on Protest**

☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.

☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.

☐ No protest accompanied the payment of additional search fees.

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

International application No.
**PCT/US2022/014430**

| Patent document cited in search report | Publication date (day/month/year) | Patent family member(s) | Publication date (day/month/year) |
|---|---|---|---|
| US 2019-0182655 A1 | 13 June 2019 | US 11184756 B2 | 23 November 2021 |
| WO 2009-016967 A1 | 05 February 2009 | CA 2687949 A1 | 05 February 2009 |
| | | CN 101690281 A | 31 March 2010 |
| | | EP 2183931 A1 | 12 May 2010 |
| | | JP 2010-533994 A | 28 October 2010 |
| | | KR 10-2010-0022530 A | 02 March 2010 |
| | | US 2010-0195570 A1 | 05 August 2010 |