



(51) International Patent Classification:
H04W 12/08 (2021.01)

(21) International Application Number:
PCT/CN2024/111114

(22) International Filing Date:
09 August 2024 (09.08.2024)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant: **ZTE CORPORATION** [CN/CN]; ZTE Plaza,
Keji Road South, Hi-Tech Industrial Park, Nanshan, Shen-
zhen, Guangdong 518057 (CN).

(72) Inventors: **LIU, Peilin**; ZTE Plaza, Keji Road South,
Hi-Tech Industrial Park, Nanshan, Shenzhen, Guangdong
518057 (CN). **YOU, Shilin**; ZTE Plaza, Keji Road South,
Hi-Tech Industrial Park, Nanshan, Shenzhen, Guangdong
518057 (CN). **LI, Zhendong**; ZTE Plaza, Keji Road South,
Hi-Tech Industrial Park, Nanshan, Shenzhen, Guangdong
518057 (CN). **LIU, Yuze**; ZTE Plaza, Keji Road South,
Hi-Tech Industrial Park, Nanshan, Shenzhen, Guangdong

518057 (CN). **XING, Zhen**; ZTE Plaza, Keji Road South,
Hi-Tech Industrial Park, Nanshan, Shenzhen, Guangdong
518057 (CN). **ZHANG, Leyi**; ZTE Plaza, Keji Road South,
Hi-Tech Industrial Park, Nanshan, Shenzhen, Guangdong
518057 (CN). **MA, Wei**; ZTE Plaza, Keji Road South,
Hi-Tech Industrial Park, Nanshan, Shenzhen, Guangdong
518057 (CN).

(74) Agent: **BEYOND ATTORNEYS AT LAW**; F6, Xijin
Centre, 39 Lianhuachi East Rd., Haidian District, Beijing
100036 (CN).

(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, CV, CZ, DE, DJ, DK, DM,
DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT,
HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG,
KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY,
MA, MD, MG, MK, MN, MU, MW, MX, MY, MZ, NA,
NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO,
RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH,

(54) Title: METHOD, DEVICE AND COMPUTER PROGRAM PRODUCT FOR WIRELESS COMMUNICATION

*receiving, via the communication unit from a wireless communication terminal, a request message
comprising a user identifier to be activated*



*transmitting, by the wireless communication node to the wireless communication terminal, a
response message indicating whether the user identifier is successfully activated or whether a
session for the user identifier is established*

FIG. 7

(57) Abstract: A wireless communication method is disclosed. The method comprises receiving, via the communication unit from a wireless communication terminal, a request message comprising a user identifier to be activated; and transmitting, by the wireless communication node to the wireless communication terminal, a response message indicating whether the user identifier is successfully activated or whether a session for the user identifier is established.



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, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, 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, ME, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

- *with international search report (Art. 21(3))*
- *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*
- *upon request of the applicant, before the expiration of the time limit referred to in Article 21(2)(a)*

Method, Device and Computer Program Product for Wireless Communication

This document is directed generally to wireless communications, and in particular to 5th generation (5G) communications or 6th generation (6G) communications.

User identifiers in a communication network help an operator to provide customization and enhanced user experience for services inside and outside the network. However, the implementation of user identifiers is still a topic to be discussed.

This document relates to methods, systems, and computer program products for a wireless communication.

One aspect of the present disclosure relates to a wireless communication method. In an embodiment, the wireless communication method includes: receiving, via the communication unit from a wireless communication terminal, a request message comprising a user identifier to be activated; and transmitting, by the wireless communication node to the wireless communication terminal, a response message indicating whether the user identifier is successfully activated or whether a session for the user identifier is established.

Another aspect of the present disclosure relates to a wireless communication method. In an embodiment, the wireless communication method includes: transmitting, via the communication unit to a wireless communication node, a request message comprising a user identifier to be activated; and receiving, by the wireless communication terminal from the wireless communication node, a response message indicating whether the user identifier is successfully activated or whether a session for the user identifier is established.

Another aspect of the present disclosure relates to a wireless communication terminal. In an embodiment, the wireless communication terminal includes a communication unit and a processor. The processor is configured for: receiving, via the communication unit from a wireless communication terminal, a request message comprising a user identifier to be activated; and transmitting, by the wireless communication node to the wireless communication terminal, a response message indicating whether the user identifier is successfully activated or whether a session for the user identifier is established.

Another aspect of the present disclosure relates to a wireless communication node. In an

embodiment, the wireless communication node includes a communication unit and a processor. The processor is configured for: transmitting, via the communication unit to a wireless communication node, a request message comprising a user identifier to be activated; and receiving, by the wireless communication terminal from the wireless communication node, a response message indicating whether the user identifier is successfully activated or whether a session for the user identifier is established.

Various embodiments may preferably implement the following features:

Preferably, the wireless communication node comprises a management node.

Preferably, the management node performs at least one of:

determining whether to activate the user identifier based on whether the user identifier in the request message matches user identifier activation information in a first message from an anchor node or an application node;

transmitting, to an anchor node or an application node, a second message comprising the user identifier and an activation result of the user identifier indicating whether the user identifier is successfully activated; or

receiving, from an application node, a third message indicating whether the user identifier is successfully activated.

Preferably, the management node performs at least one of:

receiving the first message from the application node directly, via an anchor node, or via an anchor node and a network exposure node;

transmitting the second message to the application node directly, via an anchor node, or via an anchor node and a network exposure node; or

receiving the third message from the application node directly, via an anchor node, or via an anchor node and a network exposure node.

Preferably, at least one of the first message or the third message comprises at least one of the user identifier or an identifier of the wireless communication terminal.

Preferably, the identifier of the wireless communication terminal comprises at least one of:

a Subscription Permanent Identifier, SUPI, of the wireless communication terminal; or
a Generic Public Subscription Identifier, GPSI, of the wireless communication terminal.

Preferably, the response message comprises the user identifier and an activation result of the user identifier.

Preferably, the wireless communication node comprises an anchor node.

Preferably, the anchor node performs at least one of:

transmitting, to a management node or an application node, user identifier activation information;

receiving, from a management node, the user identifier and an activation result of the user identifier;

forwarding, from an application node or a network exposure node to a management node, a first message for activating the user identifier; or

forwarding, from a management node to an application node or a network exposure node, a second message comprising the user identifier and an activation result of the user identifier.

Preferably, the anchor node acquires the user identifier activation information based on a key identifier received from an application node.

Preferably, the wireless communication node comprises an application node.

Preferably, the application node performs at least one of:

transmitting, to a management node, a first message for activating the user identifier; or

transmitting, to a management node, a third message indicating whether the user identifier is successfully activated.

Preferably, the application node transmits the first or third message in response to a decrypted user identifier matches user identifier activation information from an anchor node.

Preferably, the application node checks whether the decrypted user identifier matches the user identifier activation information based on a service type from the request message.

Preferably, the application node decrypts the request message to acquire a decrypted user identifier and/or a service type.

Preferably, the request message comprises a User Identities and Authentication, UIA, Active Request message received by a management node of the wireless communication node and/or an Application Session Establishment Request message received by an application node of the wireless communication node; and/or

wherein the response message comprises a UIA Active Response message transmitted

from a management node of the wireless communication node to the wireless communication terminal and/or an Application Session Establishment Response message transmitted from an application node of the wireless communication node to the wireless communication terminal.

Preferably, wherein a first response message of the request message transmitted to a management node of the wireless communication node comprises the user identifier and an activation result of the user identifier.

Preferably, a first request message of the request message transmitted to a management node of the wireless communication node comprises a User Identities and Authentication, UIA, Active Request message and/or a first response message of the response message received from a management node of the wireless communication node comprises a UIA Active Response message.

Preferably, a second request message of the request message transmitted to an application node of the wireless communication node further comprises a service type for activating the user identifier.

Preferably, the user identifier and/or the service type in the second request message is encrypted.

Preferably, a second request message of the request message transmitted to an application node of the wireless communication node comprises an Application Session Establishment Request message and/or a second response message of the response message received from an application node of the wireless communication node comprises an Application Session Establishment Response message.

The present disclosure relates to a computer program product comprising a computer-readable program medium code stored thereupon, the code, when executed by a processor, causing the processor to implement a wireless communication method recited in any one of foregoing methods.

The exemplary embodiments disclosed herein are directed to providing features that will become readily apparent by reference to the following description when taken in conjunction with the accompanying drawings. In accordance with various embodiments, exemplary systems, methods, devices and computer program products are disclosed herein. It is understood, however, that these embodiments are presented by way of example and not limitation, and it will be apparent to those of ordinary skill in the art who read the present disclosure that various modifications to the

disclosed embodiments can be made while remaining within the scope of the present disclosure.

Thus, the present disclosure is not limited to the exemplary embodiments and applications described and illustrated herein. Additionally, the specific order and/or hierarchy of steps or operations in the methods disclosed herein are merely exemplary approaches. Based upon design preferences, the specific order or hierarchy of steps or operations of the disclosed methods or processes can be re-arranged while remaining within the scope of the present disclosure. Thus, those of ordinary skill in the art will understand that the methods and techniques disclosed herein present various steps or operations in a sample order, and the present disclosure is not limited to the specific order or hierarchy presented unless expressly stated otherwise.

The above and other aspects and their implementations are described in greater detail in the drawings, the descriptions, and the claims.

FIG. 1A and FIG. 1B show a procedure according to an embodiment of the present disclosure.

FIG. 2 shows a schematic diagram of a procedure according to an embodiment of the present disclosure.

FIG. 3 shows a schematic diagram of a procedure according to an embodiment of the present disclosure.

FIG. 4 shows a schematic diagram of a procedure according to an embodiment of the present disclosure.

FIG. 5 shows an example of a schematic diagram of a wireless communication terminal according to an embodiment of the present disclosure.

FIG. 6 shows an example of a schematic diagram of a wireless communication node according to an embodiment of the present disclosure.

FIGs. 7 and 8 show flowcharts of wireless communication methods according to some embodiments of the present disclosure.

Some embodiments of the present disclosure, directed to User Identities and Authentication (UIA) Architecture, which enhances the 5G System (5GS) to allow for the creation and utilization of user-specific identities in order to provide the enhanced user experience, the optimized performance, and offer services to specific users. In some embodiments, one or more users (e.g., human(s) or machine(s) identified by user identifier(s) (also referred to as user id(s) in

the present disclosure)) sharing one User Equipment (UE). In some embodiments (e.g., when the user identifier applies to a human), a single user identifier is active with a UE subscription at a given time and it is assumed that the specific user identifier is associated with all of the UE's traffic during the time that specific user identifier is active with the UE's subscription. In some embodiments, a user is considered active if the associated user identifier has been authenticated and authorized to use a linked subscription to access the 5GS.

Some embodiments of the present disclosure may provide a mechanism related to a user identifier. Some embodiments of the present disclosure may provide a mechanism to active a specific user identifier (e.g., applies to a specific human).

In some embodiments, the user identifier is different from the UE identifier (also referred to as the identifier of the UE) (e.g., SUPI (Subscription Permanent Identifier) or GPSI (Generic Public Subscription Identifier)) of the associated UE (e.g., the UE operated by the user). In some embodiments, more than one user identifier may correspond to one UE identifier (e.g., the UE may be operated by different users). In some embodiments, one user identifier may correspond to more than one UE identifier (e.g., different UEs may be operated by a user).

In the paragraphs below, some aspects of the present disclosure are provided, but the present disclosure is not limited thereto. Besides, embodiments in different aspects described below can be combined or cross-referenced unless expressly stated otherwise.

Aspect 0:

FIG. 1A and FIG. 1B show a procedure for User Identifier key material sharing to a UIA Anchor according to an embodiment of the present disclosure. In some embodiments, the procedure may include at least one of the following operations.

1. The UE sends a registration request to the gNodeB (gNB), including the UE 5G-Globally Unique Temporary Identity (GUTI) or Subscription Concealed Identifier (SUCI).
2. The Radio Access Network (RAN) selects an Access and Mobility Management Function (AMF) and forwards the Registration Request to the AMF.
3. [Conditional] The new AMF sends a complete Registration Request (e.g., the Namf_Communication_UEContextTransfer) to the old AMF. In some embodiments, the new AMF determines the old AMF using the UE's 5G-GUTI.

4. [Conditional] The old AMF sends a response (e.g., the `Namf_Communication_UEContextTransfer`) to the new AMF. In some embodiments, the response includes the Subscription Permanent Identifier (SUPI) and/or the UE Context in the AMF.

5. [Conditional] The new AMF sends an identity request to the UE.

In some embodiments, if the SUCI is not provided by the UE nor retrieved from the old AMF, the Identity Request procedure is initiated by the AMF sending an Identity Request message to the UE requesting the SUCI.

6. [Conditional] The UE sends an identity response to the new AMF.

In some embodiments, the UE responds with an Identity Response message including the SUCI. The UE derives the SUCI by using the provisioned public key of the Home Public Land Mobile Network (HPLMN).

7. The AMF may invoke the service (e.g., the `Nausf_UEAuthentication`) by sending a request message (e.g., the `Nausf_UEAuthentication_Authenticate`) to the Authentication Server Function (AUSF) whenever the AMF wishes to initiate an authentication, containing SUPI/SUCI and the serving network name.

8. The AUSF sends a request (e.g., the `Nudm_UEAuthentication_Get Request`) to the Unified Data Management (UDM), including the SUCI/SUPI and the serving network name.

9. The UDM may return the 5G Home Environment Authentication Vector (HE AV) to the AUSF together with an indication that the 5G HE AV is to be used for 5G AKA in a response (e.g., the `Nudm_UEAuthentication_Get Response`). In some embodiments, in case that SUCI was included in the request (e.g., the `Nudm_UEAuthentication_Get Request`), the UDM may include the SUPI in the response (e.g., the `Nudm_UEAuthentication_Get Response`) after deconcealment of the SUCI.

In some embodiments, if a subscriber has a UIA subscription, the UDM includes the user subscription in the response (e.g., the `Nudm_UEAuthentication_Get Response`). The user subscription contains at least a user id (also referred to as `User_Id` in this disclosure) list. In some embodiments, the format of the user id is not constrained, and thus, if the UIA-AnchorID is not a partial of the user id, the user subscription sends to the AUSF also contains an UIA-AnchorID list, which has a mapping relationship with the user id list.

The UIA-AnchorID is used for the network to identify the specific UIA Anchor

Function for a specific user id. Different user ids for a single UE may have different UIA-AnchorIDs, and therefore register to different UIA Anchor Functions.

10. The AUSF may store the Expected Response (XRES*) temporarily together with the received SUCI or the received SUPI.

The AUSF may then generate the 5G AV from the 5G HE AV received from the UDM/Authentication credential Repository and Processing Function (ARPF) by computing the Expected Response (HXRES*) from the XRES* and the Security Anchor Function Key (K_{SEAF}) from the K_{AUSF} , and replacing the XRES* with the HXRES* and K_{AUSF} with K_{SEAF} in the 5G HE AV.

The AUSF may then remove the K_{SEAF} and return the 5G SE AV (Random Number (RAND), Authentication Token (AUTN), HXRES*) to the AMF in a response (e.g., the Nausf_UEAuthentication_UEAuthentication Response).

11. The AMF may send the RAND, the AUTN to the UE in a request (e.g., Non-Access Stratum (NAS) message Authentication Request). In some embodiments, this message may also include the Key Set Identifier (ngKSI) that may be used by the UE and the AMF to identify the K_{AMF} and the partial native security context that is created if the authentication is successful. This message may also include the Anti-Bidding down Between Architectures (ABBA) parameter. The AMF may set the ABBA parameter. The UE may forward the RAND and AUTN received in NAS message Authentication Request to the Universal Subscriber Identity Module (USIM).

12. At receipt of the RAND and the AUTN, the USIM may verify the freshness of the received values by checking whether the AUTN can be accepted. If the AUTN is accepted, the USIM computes a response (e.g., RES). The USIM may return the RES, the Cipher Key (CK), the Integrity Key (IK) to the UE. If the USIM computes a K_c (i.e., General Packet Radio Service (GPRS) K_c) from the CK and the IK, and sends it to the UE, then the UE may ignore such GPRS K_c and not store the GPRS K_c on the USIM or in the UE. The UE then may compute RES* from RES. The UE may calculate the K_{AUSF} from the CK||IK. The UE may calculate the K_{SEAF} from the K_{AUSF} .

The UE may return the RES* to the AMF in a response (e.g., the NAS message Authentication Response).

13. The AMF may then compute HRES* from RES*, and the AMF may compare HRES* and HXRES*. If they coincide, the AMF may consider the authentication successful from

the serving network point of view.

The AMF may send the RES*, as received from the UE, in a request (e.g., the Nausf_UEAuthentication_Authenticate Request message) to the AUSF.

14. When the AUSF receives as authentication confirmation the request (e.g., the Nausf_UEAuthentication_Authenticate Request message) including a RES*, it may verify whether the 5G AV has expired. If the 5G AV has expired, the AUSF may consider the authentication as unsuccessful from the home network point of view. Upon successful authentication, the AUSF stores the K_{AUSF} based on the home network operator's policy. The AUSF may compare the received RES* with the stored XRES*. If the RES* and XRES* are equal, the AUSF may consider the authentication as successful from the home network point of view.

The AUSF may indicate to the AMF in the response (e.g., the Nausf_UEAuthentication_Authenticate Response) whether the authentication was successful or not from the home network point of view. If the authentication was successful, the K_{SEAF} may be sent to the SEAF in the response (e.g., the Nausf_UEAuthentication_Authenticate Response). In case the AUSF received a SUCI from the SEAF in the authentication request, and if the authentication was successful, then the AUSF may also include the SUPI in the response (Nausf_UEAuthentication_Authenticate Response message).

The AUSF includes the received user id list in the response (e.g., Nausf_UEAuthentication_Authenticate Response message).

15-16. The AMF and the UE complete the NAS security mode command procedure to establish NAS Security context between the UE and the AMF.

17a-17b. If the AUSF receives the user id list from the UDM, the AUSF stores the K_{AUSF} and generate the UIA Anchor Key (K_{UIA}) and the UIA-KID based on K_{AUSF} after the primary authentication procedure is successfully completed.

The UE generates the UIA Anchor Key (K_{UIA}) and the UIA-KID based on K_{AUSF} before initiating communication with an UIA Application Function.

17c. After UIA key material is generated, the AUSF selects the UIA-Anchor Function (also referred to as UIA-Anchor) according to the UIA-AnchorID or the user id, and sends the generated UIA-KID and K_{UIA} to the UIA-Anchor Function together with the user id using the service operation (e.g., the Nuiiaa_UIA_KeyRegistration Request service operation). If there are

more than one user ids related with the UIA-Anchor Function, the user id may be a user id list. The AUSF can optionally also send the SUPI to the UIA-Anchor Function.

The UIA-Anchor Function stores the latest information sent by the AUSF.

17d. The UIA-Anchor Function sends the response to the AUSF using the service operation (e.g., Nuiiaa_UIA_AnchorKey_Register Response service operation).

18. The new AMF registers with the UDM using a registration (e.g., Nudm_UECM_Registration) for the access to be registered.

After AMF has successfully completed the operation (e.g., Nudm_UECM_Registration operation) and if the AMF does not have subscription data for the UE, the AMF retrieves the Access and Mobility Subscription data, the SMF Selection Subscription data, the UE context in the SMF data and the Location services (LCS) mobile origination using a service operation request (e.g., Nudm_SDM_Get).

After a successful response is received, the AMF subscribes to be notified using Nudm_SDM_Subscribe when the data requested is modified.

The UDM initiates a Nudm_UECM_DeregistrationNotification to the old AMF corresponding to the same access, if one exists.

If old AMF does not have UE context for another access type (i.e. non-3GPP access), the Old AMF unsubscribes with the UDM for subscription data using Nudm_SDM_unsubscribe.

19. The new AMF sends a registration accept to the UE.

20. The UE sends a registration complete to the new AMF.

Aspect 1:

In some embodiments, before the start of the communication between the UE and the UIA Application Function (UIA AF), the UE and the UIA AF may know whether to implement the mechanism of the user identifier. This knowledge can be obtained from an application on the UE and/or the UIA AF or indicated from the network (e.g., from the UIA AF) to the UE.

FIG. 2 shows a user identifier activation procedure according to an embodiment of the present disclosure. In some embodiments, the UDM performs the user identifier activation. In some embodiments, the procedure may include at least one of the following operations.

1. The UE may be registered and established PDU Sessions. In some embodiments,

the registration can be performed by using the procedure described in Aspect 0, and details in this regard will not be repeated herein. In some embodiments, the registration can be performed by using another registration procedure.

2a. If a user id (e.g., the User_Id#1, in the paragraph below, User_Id#1 will be taken as an example, but the present disclosure is not limited thereto) intends to use the UE, the UE may send a request (e.g., the UIA Active request, in the paragraph below, the UIA Active request will be taken as an example, but the present disclosure is not limited thereto) to the AMF with the user id (e.g., the User_Id#1). In some embodiments, the AMF forwards the request to the UDM.

2b. The UE transmits another request (e.g., the Application Session Establishment Request message) to an UIA AF. In some embodiments, said another request comprises the UIA-KID and the user id. In some embodiments, the user id is encrypted. In some embodiments, the user id is encrypted by a key K_{UIAAF} (e.g., a key used for the communication between the UE and the UIA AF). In some embodiments, the UE derives K_{UIAAF} from the UIA Anchor Key (K_{UIA}). In some embodiments, the UE generates the UIA Anchor Key (K_{UIA}) and/or the UIA-KID based the K_{AUSF} (e.g., before initiating the communication with the UIA AF).

3. If the UIA AF does not have an active context associated with the UIA-KID, the UIA AF selects the UIA-Anchor Function, and sends a request (e.g., Nuiaa_UIA_ApplicationKey_Get request) to the UIA-Anchor Function with the UIA-KID to request the K_{UIAAF} for the UE. In some embodiments, the UIA AF also includes its identity (UIA_AF_ID) in the request (e.g., Nuiaa_UIA_ApplicationKey_Get request).

In some embodiments, the UIA-Anchor Function checks whether the UIA-Anchor Function can provide the service to the UIA AF based on the configured local policy or based on the authorization information available in the signaling (i.e., Oauth2.0 token). If it succeeds, the following procedures are executed. Otherwise, the UIA-Anchor Function rejects the procedure.

In some embodiments, the Authentication and Key Management for Applications (AKMA) Anchor Function (AAnF) verifies whether the subscriber is authorized to use UIA based on the presence of the UE specific K_{UIA} key identified by the UIA-KID.

If K_{UIA} is present in UIA-Anchor Function, the UIA-Anchor Function continues with operation 4.

If K_{UIA} is not present in the UIA-Anchor Function, the UIA-Anchor Function continues

with operation 9 with an error response (e.g., the UIA-Anchor Function transmits an error response to the UIA AF in operation 9).

4. The UIA-Anchor Function derives the UIA Application Key (K_{UIAAF}) based on K_{UIA} if it does not already have K_{UIAAF} .

5. The UIA-Anchor Function transmits a request (e.g., the Nudm_UIA_Active request message) to the UDM. In some embodiments, the request comprises user identifier activation information (e.g., the user id). In some embodiments, the UIA-Anchor Function acquires the user identifier activation information based on the received UIA-KID. In some embodiments, an identifier (e.g., the SUPI) of the UE may also be included in the request.

6. The UDM determines whether to activate the user id (e.g., User_Id#1). In some embodiments, the UDM determines whether to activate the user id based on whether the user id received in operation 2a matches the user identifier activation information received in operation 5. In some embodiments, when the user identifier activation information includes or is a user id, the UDM determines whether to activate the user id based on whether the user id received in operation 2a and the user id received in operation 5 identifier the same user of the UE. In some embodiments, if the user id received in operation 2a matches the user identifier activation information received in operation 5, the UDM activates this user id (e.g., the User_Id#1). In some embodiments, if the user id received in operation 2a matches the user identifier activation information received in operation 5, the UDM determines the user identifier activation is failed and does not activate the user id.

7. The UDM sends the response (e.g., the UIA active response) to the AMF. In some embodiments, the response includes at least one of the user id (e.g., User_Id#1) and/or the activation result indicating whether the user identifier is successfully activated. In some embodiments, the AMF forwards the response to the UE.

8. The UDM sends another response (e.g., the Nudm_UIA_Active response) to the UIA-Anchor. In some embodiments, the response includes at least one of the user id (e.g., User_Id#1) and/or the activation result.

9. The UIA-Anchor Function sends the response (e.g., Nniaa_UIA_ApplicationKey_Get response) to the UIA AF including at least one of the user id (e.g., User_Id#1) the GPSI or SUPI, K_{UIAAF} and/or the K_{UIAAF} expiration time. In some embodiments, whether to send the SUPI or the GPSI is determined by the UIA-Anchor Function

based on the local policy.

10. The UIA AF uses the received K_{UIAAF} to get the plain text of the user id (e.g., User_Id#1). The UIA AF then performs the user id (e.g., User_Id#1) based Extensible Authentication Protocol (EAP) authentication with the Authentication, Authorization, and Accounting Server (AAA-S). The UIA AF may check whether the plain text user id (e.g., User_Id#1) matches with the user id (e.g., User_Id#1) received from UIA-Anchor.

11. The UIA AF sends the response (e.g., Application Session Establishment Response) to the UE. If the information in operation 9 indicates a failure, the UIA AF rejects the Application Session Establishment by including a failure cause.

Details can be ascertained by referring to the embodiments in Aspect 0 above, and will not be repeated herein.

Aspect 2:

In some embodiments, before the start of the communication between the UE and the UIA Application Function (UIA AF), the UE and the UIA AF may know whether to implement the mechanism of the user identifier. This knowledge can be obtained from an application on the UE and/or the UIA AF or indicated from the network (e.g., from the UIA AF) to the UE.

FIG. 3 shows a user identifier activation procedure according to an embodiment of the present disclosure. In some embodiments, both the UIA AF and the UDM are involved in the user identifier activation. In some embodiments, the procedure may include at least one of the following operations.

1. The UE is registered and established PDU Sessions. In some embodiments, the registration can be performed by using the procedure described in Aspect 0, and details in this regard will not be repeated herein. In some embodiments, the registration can be performed by using another registration procedure.

2a. If a user id (e.g., the User_Id#1) intends to use the UE, the UE may send a request (e.g., the UIA Active request, in the paragraph below) to the AMF with the user id (e.g., the User_Id#1). In some embodiments, the AMF forwards the request to the UDM.

2b. The UE transmits another request (e.g., the Application Session Establishment Request message) to an UIA AF. In some embodiments, said another request comprises the UIA-KID and the user id. In some embodiments, said another request further comprises a service type.

In some embodiments, the service type may be set to “activate” or “active”. In some embodiments, the service type may be used to request the activation of the user id. In some embodiments, the user id and/or the service type is encrypted. In some embodiments, the user id and/or the service type is encrypted by a key K_{UIAAF} . In some embodiments, the UE derives K_{UIAAF} from the UIA Anchor Key (K_{UIA}). In some embodiments, the UE generates the UIA Anchor Key (K_{UIA}) and/or the UIA-KID based the K_{AUSF} (e.g., before initiating the communication with the UIA AF).

3. If the UIA AF does not have an active context associated with the UIA-KID, the UIA AF selects the UIA-Anchor Function, and sends a request (e.g., `Nuiaa_UIA_ApplicationKey_Get` request) to the UIA-Anchor Function with the UIA-KID to request the K_{UIAAF} for the UE. In some embodiments, the UIA AF also includes its identity (`UIA_AF_ID`) in the request.

In some embodiments, the UIA-Anchor Function checks whether the UIA-Anchor Function can provide the service to the UIA AF based on the configured local policy or based on the authorization information available in the signaling (i.e., OAuth2.0 token). If it succeeds, the following procedures are executed. Otherwise, the UIA-Anchor Function rejects the procedure.

In some embodiments, the AAnF verifies whether the subscriber is authorized to use UIA based on the presence of the UE specific K_{UIA} key identified by the UIA-KID.

In some embodiments, if K_{UIA} is present in the UIA-Anchor Function, the UIA-Anchor Function continues with operation 4.

In some embodiments, if K_{UIA} is not present in the UIA-Anchor Function, the UIA-Anchor Function continues with operation 5 with an error response (e.g., the UIA-Anchor Function transmits an error response to the UIA AF in operation 5).

4. The UIA-Anchor Function derives the UIA Application Key (K_{UIAAF}) based on K_{UIA} if it does not already have K_{UIAAF} .

5. The UIA-Anchor Function sends a response (e.g., `Nniaa_UIA_ApplicationKey_Get` response) to the UIA AF. In some embodiments, the request comprises the user identifier activation information (e.g., including the user id (e.g., `User_Id#1`)), an identifier of the UE (e.g., SUPI or GPSI), K_{UIAAF} and/or the K_{UIAAF} expiration time. In some embodiments, the UIA-Anchor Function acquires the user identifier activation information based on the received UIA-KID. In some embodiments, whether to send the SUPI or the GPSI is

determined by UIA-Anchor Function based on the local policy.

6. The UIA AF decrypts the request received in operation 2b to get the plain text of User_Id#1 and/or service type. In some embodiments, the UIA AF decrypts the request received in operation 2b using the received K_{UIAAF} . In some embodiments, the UIA AF checks whether the decrypted user id (e.g., the plain text of User_Id#1) matches the user identifier activation information based on a service type from the request message. In some embodiments, the UIA AF checks whether the decrypted user id matches the user identifier activation information in response to the service type is “active”. In some embodiments, when the user identifier activation information includes or is a user id, the UIA AF checks whether the decrypted user id and the user id received in operation 5 identify the same user. In some embodiments, if the decrypted user id matches the user identifier activation information received from UIA-Anchor in operation 5, the UIA AF performs operation 7. In some embodiments, if the decrypted user id matches the user identifier activation information, the UIA AF performs the user id based EAP authentication with the AAA-S.

7. The UIA AF sends a request (e.g., the UIA Active request) user identifier activation information (e.g., including User_Id#1) (e.g., can be the one received from the UIA-Anchor in operation 5 or different user identifier activation information to the UDM. In some embodiments, the request may further include the UE identifier. In some embodiments, there are some options (as described in operations 7a to 7c) to sends the request to the UDM.

7a. The UIA AF sends the request (e.g., the Nuiaa_UIA_Active request) to the UIA-Anchor with the user identifier activation information (e.g., including User_Id#1) and optionally with the SUPI. In some embodiments, the UIA-Anchor sends the request (e.g., the Nudm_UIA_Active request) to the UDM.

7b. The UIA AF sends the request (e.g., the Nudm_UIA_Active request) to the UDM with the user identifier activation information (e.g., including User_Id#1) and optionally with the SUPI. In some embodiments, the UIA AF directly sends the request to the UDM.

7c. If the UIA AF is outside the operator domain, the UIA AF sends the request (e.g., the Nnef_UIA_Active request) to the NEF with the user identifier activation information (e.g., including User_Id#1) and optionally with the GPSI. In some embodiments, the NEF then forwards the request to the UDM through the UIA-Anchor.

8. The UDM determines whether to activate the user id (e.g., User_Id#1). In some embodiments, the UDM determines whether to activate the user id based on whether the user id received in operation 2a matches the user identifier activation information received in operation 7. In some embodiments, when the user identifier activation information includes or is a user id, the UDM determines whether to activate the user id based on whether the user id received in operation 2a and the user id received in operation 7 identifier the same user of the UE. In some embodiments, if the user id received in operation 2a matches the user identifier activation information received in operation 7, the UDM activates this user id (e.g., the User_Id#1). In some embodiments, if the user id received in operation 2a matches the user identifier activation information received in operation 7, the UDM determines the activation for the user identifier is failed and does not activate the user id.

In some embodiments, the UDM sends a response (e.g., the UIA Active response) to the UIA AF. In some embodiments, the response includes at least one of the user id (e.g., the User_Id#1) and/or the activation result. In some embodiments, there are some options (as described in operations 8a to 8c below) to sends the request to the UIA AF.

8a. The UDM sends the response to the UIA AF via the UIA-Anchor.

8b. The UDM directly sends the response to the UIA AF.

8c. If the UIA AF is outside the operator domain, the UDM sends the response to the UIA AF via the NEF and the UIA-Anchor.

9. The UDM sends another response (e.g., the UIA active response) to the AMF with the user id (e.g., User_Id#1) and the activation result. In some embodiments, the AMF forwards the response to the UE.

10. The UIA AF sends the response (e.g., the Application Session Establishment Response) to the UE. If the UIA AF receives the error response in operation 5 or the response received in operation 8 indicates the activation of the user id is failed, the UIA AF rejects the request (e.g., the Application Session Establishment) by including a failure cause.

Details can be ascertained by referring to the embodiments in Aspect 0 and Aspect 1 above, and will not be repeated herein.

Aspect 3:

In some embodiments, before the start of the communication between the UE and the

UIA Application Function (UIA AF), the UE and the UIA AF may know whether to implement the mechanism of the user identifier. This knowledge can be obtained from an application on the UE and/or the UIA AF or indicated from the network (e.g., from the UIA AF) to the UE.

FIG. 4 shows a user identifier activation procedure according to an embodiment of the present disclosure. In some embodiments, the UIA AF (e.g., the application layer) performs the user identifier activation and informs the UDM. In some embodiments, the procedure may include at least one of the following operations.

1. The UE may be registered and established PDU Sessions. In some embodiments, the registration can be performed by using the procedure described in Aspect 0, and details in this regard will not be repeated herein. In some embodiments, the registration can be performed by using another registration procedure.

2. If the user id (e.g., the User_Id#1) intends to use the UE, the UE sends a request (e.g., the Application Session Establishment Request message) to an UIA AF. In some embodiments, the request comprises the UIA-KID and the user id. In some embodiments, the request further comprises a service type. In some embodiments, the service type may be set to “activate” or “active”. In some embodiments, the service type may be used to request the activation of the user id. In some embodiments, the user id and/or the service type is encrypted. In some embodiments, the user id and/or the service type is encrypted by a key K_{UIAAF} . In some embodiments, the UE derives K_{UIAAF} from the UIA Anchor Key (K_{UIA}). In some embodiments, the UE generates the UIA Anchor Key (K_{UIA}) and/or the UIA-KID based the K_{AUSF} (e.g., before initiating the communication with the UIA AF).

3. If the UIA AF does not have an active context associated with the UIA-KID, the UIA AF selects the UIA-Anchor Function and sends a request (e.g., the Nuiaa_UIA_ApplicationKey_Get request) to the UIA-Anchor Function with the UIA-KID to request the K_{UIAAF} for the UE. In some embodiments, the UIA AF also includes its identity (UIA_AF_ID) in the request.

In some embodiments, the UIA-Anchor Function checks whether the UIA-Anchor Function can provide the service to the UIA AF based on the configured local policy or based on the authorization information available in the signaling (i.e., Oauth2.0 token). If it succeeds, the following procedures are executed. Otherwise, the UIA-Anchor Function rejects the procedure.

In some embodiments, the AAnF verifies whether the subscriber is authorized to use UIA based on the presence of the UE specific K_{UIA} key identified by the UIA-KID.

In some embodiments, if K_{UIA} is present in UIA-Anchor Function, the UIA-Anchor Function continues with operation 4.

If K_{UIA} is not present in the UIA-Anchor Function, the UIA-Anchor Function continues with operation 5 with an error response (e.g., the UIA-Anchor Function transmits an error response to the UIA AF in operation 5).

4. The UIA-Anchor Function derives the UIA Application Key (K_{UIAAF}) based on K_{UIA} if it does not already have K_{UIAAF} .

5. The UIA-Anchor Function sends a response (e.g., Nniaa_UIA_ApplicationKey_Get response) to the UIA AF. In some embodiments, the request comprises the user identifier activation information (e.g., including the user id (e.g., User_Id#1)), an identifier of the UE (e.g., SUPI or GPSI), K_{UIAAF} and/or the K_{UIAAF} expiration time. In some embodiments, the UIA-Anchor Function acquires the user identifier activation information based on the received UIA-KID. In some embodiments, whether to send the SUPI or the GPSI is determined by the UIA-Anchor Function based on the local policy.

6. The UIA AF decrypts the request received in operation 2b to get the plain text of User_Id#1 and/or service type. In some embodiments, the UIA AF decrypts the request received in operation 2b using the received K_{UIAAF} . In some embodiments, the UIA AF checks whether the decrypted user id (e.g., the plain text of User_Id#1) matches the user identifier activation information based on a service type from the request message. In some embodiments, the UIA AF checks whether the decrypted user id matches the user identifier activation information in response to the service type is “active”. In some embodiments, when the user identifier activation information includes or is a user id, the UIA AF checks whether the decrypted user id and the user id received in operation 5 identify the same user. In some embodiments, if the decrypted user id matches the user identifier activation information received from UIA-Anchor in operation 5, the UIA AF performs operation 7. In some embodiments, if the decrypted user id matches the user identifier activation information, the UIA AF performs the user id based EAP authentication with the AAA-S.

7. The UIA AF sends a notification (e.g., the Nudm_UIA Active Notify) to the

UDM inform the UDM that the User_Id#1 is activated. In some embodiments, the notification may include at least one of the user id (e.g., the User_Id#1) and/or the UE identifier. In some embodiments, there are some options (as described in operations 7a to 7c) to sends the request to the UDM.

7a. The UIA AF sends the notification to the UDM via the UIA-Anchor.

7b. The UIA AF sends the notification to the UDM directly.

7c. If the UIA AF is outside the operator domain, the UIA AF sends the notification to the UDM via the NEF and the UIA-Anchor.

8. The UIA AF sends the response (e.g., Application Session Establishment Response) to the UE. If the UIA AF receives the error response in operation 5 or, in operation 6, the decrypted user id does not match the user identifier activation information received from UIA-Anchor, the UIA AF rejects the request (e.g., Application Session Establishment) by including a failure cause.

Details can be ascertained by referring to the embodiments in Aspects 0 to 2 above, and will not be repeated herein.

In some embodiments, the UDM may perform at least one of the following:

receiving the request (e.g., the UIA active request) from the AMF/UIA-Anchor/UIA AF with the user id;

checking whether the user id can be activated;

checking whether the user id matches the user identifier activation information; and/or

sending a response (e.g., the UIA active response) to the AMF/UIA-Anchor/UIA AF with the user id and the result; and/or

receiving a notification (e.g., Nudm_UIA Active Notify) from the UIA AF with the user id and/or the UE identifier.

In some embodiments, the UIA-Anchor may perform at least one of the following:

sending a request (e.g., the UIA active request) to the UDM with the user id;

receiving a response (e.g., the UIA active response) from the UDM with the user id and activation result; and/or

sending the user id to the UIA AF in the response (e.g., UIA_ApplicationKey_Get Response).

In some embodiments, the UIA AF may perform at least one of the following:

receiving the encrypted service type from the UE;

decrypting the service type;

checking whether the user id can be activated;

checking whether the user id matches the user identifier activation information;

sending a request (e.g., the UIA active request) to the UIA-Anchor/UDM/NEF with the user id and the UE identity;

receiving the response (e.g., the UIA active response) from the UIA-Anchor/UDM/NEF with the user id (e.g., User_Id#1) and the activation result; and/or

sending a notification (e.g., Nudm_UIA Active Notify) to the UDM with the user id and/or the UE identifier.

In some embodiments, the UE may perform at least one of the following:

sending a request (e.g., the UIA active request) to the AMF with the user id;

setting the service type to “active” or “activate” and encrypting the service type using the K_{UIAAF} ; and/or

sending encrypted service type to the UIA AF during the session establishment. receives a response (e.g., the UIA active response) from the AMF.

In some embodiments, the AMF forwards the messages (e.g., UIA Active Request and UIA Active Response) between the UE and the UDM.

FIG. 5 relates to a diagram of a wireless communication terminal 30 according to an embodiment of the present disclosure. The wireless communication terminal 30 may be a tag, a mobile phone, a laptop, a tablet computer, an electronic book or a portable computer system and is not limited herein. The wireless communication terminal 30 may be used to implement the UE described in this disclosure. The wireless communication terminal 30 may include a processor 300 such as a microprocessor or Application Specific Integrated Circuit (ASIC), a storage unit 310 and a communication unit 320. The storage unit 310 may be any data storage device that stores a program code 312, which is accessed and executed by the processor 300. Embodiments of the storage unit 310 include but are not limited to a subscriber identity module (SIM), read-only memory (ROM), flash memory, random-access memory (RAM), hard-disk, and optical data storage device. The communication unit 320 may a transceiver and is used to transmit and receive

signals (e.g., messages or packets) according to processing results of the processor 300. In an embodiment, the communication unit 320 transmits and receives the signals via at least one antenna 322 or via wiring.

In an embodiment, the storage unit 310 and the program code 312 may be omitted and the processor 300 may include a storage unit with stored program code.

The processor 300 may implement any one of the steps or operations in exemplified embodiments on the wireless communication terminal 30, e.g., by executing the program code 312.

The communication unit 320 may be a transceiver. The communication unit 320 may as an alternative or in addition be combining a transmitting unit and a receiving unit configured to transmit and to receive, respectively, signals to and from a wireless communication node.

In some embodiments, the wireless communication terminal 30 may be used to perform the operations of the UE described in this disclosure. In some embodiments, the processor 300 and the communication unit 320 collaboratively perform the operations described in this disclosure. For example, the processor 300 performs operations and transmit or receive signals, message, and/or information through the communication unit 320.

FIG. 6 relates to a diagram of a wireless communication node 40 according to an embodiment of the present disclosure. The wireless communication node 40 may be a satellite, a base station (BS), a gNB, a network entity, a Domain Name System (DNS) server, a Mobility Management Entity (MME), Serving Gateway (S-GW), Packet Data Network (PDN) Gateway (P-GW), a radio access network (RAN), a next generation RAN (NG-RAN), a data network, a core network, a communication node in the core network, or a Radio Network Controller (RNC), and is not limited herein. In addition, the wireless communication node 40 may include (perform) at least one network function such as an access and mobility management function (AMF), a Unified Data Management (UDM), a UIA Anchor, a session management function (SMF), a user place function (UPF), a policy control function (PCF), an application function (AF) (e.g., a UIA AF), etc. The wireless communication node 40 may be a network or a network node include (perform) at least one of the UDM, the UIA-Anchor, the UIA AF, and/or the AMF described in this disclosure. The wireless communication node 40 may be used to implement the UDM, the UIA-Anchor, the UIA AF, and/or the AMF described in this disclosure or the wireless communication node 40 may be used to implement a network or a network node including at least one of the UDM, the UIA-

Anchor, the UIA AF, and/or the AMF described in this disclosure. The wireless communication node 40 may include one or more processors 400 such as a microprocessors or ASICs, one or more storage units 410 and one or more communication units 420. The storage units 410 may be any data storage devices that store one or more program codes 412, which are accessed and executed by the one or more processors 400. Examples of the one or more storage units 410 include but are not limited to a SIM, ROM, flash memory, RAM, hard-disk, and optical data storage device. The one or more communication units 420 may be transceivers and are used to transmit and receive signals (e.g., messages or packets) according to processing results of the one or more processors 400. In an embodiment, the one or more communication units 420 transmit and receive the signals via at least one antenna 422 or via wiring.

In an embodiment, the one or more storage units 410 and the one or more program codes 412 may be omitted. The one or more processors 400 may include one or more storage units with stored program codes.

The one or more processors 400 may implement any steps or operations described in exemplified embodiments on the wireless communication node 40, e.g., via executing the program codes 412.

The one or more communication units 420 may be one or more transceivers. The one or more communication units 420 may as an alternative or in addition be combining a transmitting unit and a receiving unit configured to transmit and to receive, respectively, signals, messages, or information to and from a wireless communication node or a wireless communication terminal.

In some embodiments, the wireless communication node 40 may be used to perform the operations of at least one of the UDM, the UIA-Anchor, the UIA AF, and/or the AMF described in this disclosure. In some embodiments, the one or more processors 400 and the one or more communication units 420 collaboratively perform the operations described in this disclosure. For example, the one or more processors 400 perform operations and transmit or receive signals through the one or more communication units 420. In some embodiments, different processors 400 and different communication units 420 may be used to perform operations of different network functions (e.g., the at least one of the UDM, the UIA-Anchor, the UIA AF, and/or the AMF described in this disclosure)

A wireless communication method is also provided according to an embodiment of the

present disclosure. In an embodiment, the wireless communication method may be performed by using a wireless communication terminal (e.g., a UE). In an embodiment, the wireless communication terminal may be implemented by using the wireless communication terminal 30 described in this disclosure, but is not limited thereto.

Referring to FIG. 7, in an embodiment, the wireless communication method includes: receiving, via the communication unit from a wireless communication terminal, a request message comprising a user identifier to be activated; and transmitting, by the wireless communication node to the wireless communication terminal, a response message indicating whether the user identifier is successfully activated or whether a session for the user identifier is established.

Details in this regard can be ascertained with reference to the paragraphs above, and will not be repeated herein.

Another wireless communication method is also provided according to an embodiment of the present disclosure. In an embodiment, the wireless communication method may be performed by using a wireless communication node (e.g., a UDM, a UIA-Anchor, a UIA AF, an AMF, and/or a network or network node including at least one of a UDM, a UIA-Anchor, a UIA AF and/or an AMF). In an embodiment, the wireless communication node may be implemented by using the wireless communication node 40 described in this disclosure, but is not limited thereto.

Referring to FIG. 8, in an embodiment, the wireless communication method includes: transmitting, via the communication unit to a wireless communication node, a request message comprising a user identifier to be activated; and receiving, by the wireless communication terminal from the wireless communication node, a response message indicating whether the user identifier is successfully activated or whether a session for the user identifier is established.

Details in this regard can be ascertained with reference to the paragraphs above, and will not be repeated herein.

In some embodiments, the wireless communication terminal used in the present disclosure may indicate the UE described above.

In some embodiments, the wireless communication node used in the present disclosure may indicate the UDM, the UIA-Anchor, the UIA AF, the AMF, and/or a network or network node including at least one of the UDM, the UIA-Anchor, the UIA AF, and/or the AMF described above.

In some embodiments, the management node used in the present disclosure may indicate

the UDM described above.

In some embodiments, the anchor node used in the present disclosure may indicate the UIA-Anchor described above.

In some embodiments, the application node used in the present disclosure may indicate the UIA AF described above.

In some embodiments, the network exposure node used in the present disclosure may indicate the NEF described above.

In some embodiments, the first message used in the present disclosure may indicate Nudm_UIA_Active Request in operation 5 of Aspect 1 or operation 7 in Aspect 2 described above.

In some embodiments, the second message used in the present disclosure may indicate Nudm_UIA_Active Response in operation 8 of Aspect 1 or UIA Active Response in operation 8 of Aspect 2 described above.

In some embodiments, the third message used in the present disclosure may indicate Nudm_UIA Active Notify in operation 7 of Aspect 3 described above.

In some embodiments, the key identifier used in the present disclosure may indicate UIA-KID described above.

While various embodiments of the present disclosure have been described above, it should be understood that they have been presented by way of example only, and not by way of limitation. Likewise, the various diagrams may depict an example architecture or configuration, which are provided to enable persons of ordinary skill in the art to understand exemplary features and functions of the present disclosure. Such persons would understand, however, that the present disclosure is not restricted to the illustrated example architectures or configurations, but can be implemented using a variety of alternative architectures and configurations. Additionally, as would be understood by persons of ordinary skill in the art, one or more features of one embodiment can be combined with one or more features of another embodiment described herein. Thus, the breadth and scope of the present disclosure should not be limited by any one of the above-described exemplary embodiments.

It is understood that, in the present disclosure, the term “and/or” or symbol “/” may

include any and all combinations of one or more of the associated listed items. For example, A and/or B and/or C includes any and all combinations of one or more of A, B, and C, including A, B, C, A and B, A and C, B and C, and a combination of A and B and C. Likewise, A/B/C includes any and all combinations of one or more of A, B, and C, including A, B, C, A and B, A and C, B and C, and a combination of A and B and C.

It is also understood that any reference to an element herein using a designation such as "first," "second," and so forth does not generally limit the quantity or order of those elements. Rather, these designations can be used herein as a convenient means of distinguishing between two or more elements or instances of an element. Thus, a reference to first and second elements does not mean that only two elements can be employed, or that the first element must precede the second element in some manner.

Additionally, a person having ordinary skill in the art would understand that information and signals can be represented using any one of a variety of different technologies and techniques. For example, data, instructions, commands, information, signals, bits and symbols, for example, which may be referenced in the above description can be represented by voltages, currents, electromagnetic waves, magnetic fields or particles, optical fields or particles, or any combination thereof.

A skilled person would further appreciate that any one of the various illustrative logical blocks, units, processors, means, circuits, methods and functions described in connection with the aspects disclosed herein can be implemented by electronic hardware (e.g., a digital implementation, an analog implementation, or a combination of the two), firmware, various forms of program or design code incorporating instructions (which can be referred to herein, for convenience, as "software" or a "software unit"), or any combination of these techniques.

To clearly illustrate this interchangeability of hardware, firmware and software, various illustrative components, blocks, units, circuits, operations, and steps have been described above generally in terms of their functionality. Whether such functionality is implemented as hardware, firmware or software, or a combination of these techniques, depends upon the particular application and design constraints imposed on the overall system. Skilled artisans can implement the described functionality in various ways for each particular application, but such implementation decisions do not cause a departure from the scope of the present disclosure. In accordance with various

embodiments, a processor, device, component, circuit, structure, machine, unit, etc. can be configured to perform one or more of the functions described herein. The term “configured to” or “configured for” as used herein with respect to a specified operation or function refers to a processor, device, component, circuit, structure, machine, unit, etc. that is physically constructed, programmed and/or arranged to perform the specified operation or function.

Furthermore, a skilled person would understand that various illustrative logical blocks, units, devices, components and circuits described herein can be implemented within or performed by an integrated circuit (IC) that can include a general-purpose processor, a digital signal processor (DSP), an application specific integrated circuit (ASIC), a field programmable gate array (FPGA) or other programmable logic device, or any combination thereof. The logical blocks, units, and circuits can further include antennas and/or transceivers to communicate with various components within the network or within the device. A general-purpose processor can be a microprocessor, but in the alternative, the processor can be any conventional processor, controller, or state machine. A processor can also be implemented as a combination of computing devices, e.g., a combination of a DSP and a microprocessor, a plurality of microprocessors, one or more microprocessors in conjunction with a DSP core, or any other suitable configuration to perform the functions described herein. If implemented in software, the functions can be stored as one or more instructions or code on a computer-readable medium. Thus, the steps or operations of a method or algorithm disclosed herein can be implemented as software stored on a computer-readable medium.

Computer-readable media includes both computer storage media and communication media including any medium that can be enabled to transfer a computer program or code from one place to another. A storage media can be any available media that can be accessed by a computer. By way of example, and not limitation, such computer-readable media can include RAM, ROM, EEPROM, CD-ROM or other optical disk storage, magnetic disk storage or other magnetic storage devices, or any other medium that can be used to store desired program code in the form of instructions or data structures and that can be accessed by a computer.

In this document, the term "unit" as used herein, refers to software, firmware, hardware, and any combination of these elements for performing the associated functions described herein. Additionally, for purpose of discussion, the various units are described as discrete units; however, as would be apparent to one of ordinary skill in the art, two or more units may be combined to form

a single unit that performs the associated functions according to embodiments of the present disclosure.

Additionally, memory or other storage, as well as communication components, may be employed in embodiments of the present disclosure. It will be appreciated that, for clarity purposes, the above description has described embodiments of the present disclosure with reference to different functional units and processors. However, it will be apparent that any suitable distribution of functionality between different functional units, processing logic elements or domains may be used without detracting from the present disclosure. For example, functionality illustrated to be performed by separate processing logic elements, or controllers, may be performed by the same processing logic element, or controller. Hence, references to specific functional units are only references to a suitable means for providing the described functionality, rather than indicative of a strict logical or physical structure or organization.

Various modifications to the implementations described in this disclosure will be readily apparent to those skilled in the art, and the general principles defined herein can be applied to other implementations without departing from the scope of the claims. Thus, the disclosure is not intended to be limited to the implementations shown herein, but is to be accorded the widest scope consistent with the novel features and principles disclosed herein, as recited in the claims below.

C L A I M S

1. A wireless communication method comprising:
receiving, by a wireless communication node from a wireless communication terminal, a request message comprising a user identifier to be activated; and
transmitting, by the wireless communication node to the wireless communication terminal, a response message indicating whether the user identifier is successfully activated or whether a session for the user identifier is established.
2. The wireless communication method of claim 1, wherein the wireless communication node comprises a management node, and the management node performs at least one of:
determining whether to activate the user identifier based on whether the user identifier in the request message matches user identifier activation information in a first message from an anchor node or an application node;
transmitting, to an anchor node or an application node, a second message comprising the user identifier and an activation result of the user identifier indicating whether the user identifier is successfully activated; or
receiving, from an application node, a third message indicating whether the user identifier is successfully activated.
3. The wireless communication method of claim 2, wherein the management node performs at least one of:
receiving the first message from the application node directly, via an anchor node, or via an anchor node and a network exposure node;
transmitting the second message to the application node directly, via an anchor node, or via an anchor node and a network exposure node; or
receiving the third message from the application node directly, via an anchor node, or via an anchor node and a network exposure node.
4. The wireless communication method of claim 2 or 3, wherein at least one of the first

message or the third message comprises at least one of the user identifier or an identifier of the wireless communication terminal.

5. The wireless communication method of claim 4, wherein the identifier of the wireless communication terminal comprises at least one of:
a Subscription Permanent Identifier, SUPI, of the wireless communication terminal; or
a Generic Public Subscription Identifier, GPSI, of the wireless communication terminal.
6. The wireless communication method of any of claims 2 to 5, wherein the response message comprises the user identifier and an activation result of the user identifier.
7. The wireless communication method of any of claims 1 to 6, wherein the wireless communication node comprises an anchor node, and the anchor node performs at least one of:
transmitting, to a management node or an application node, user identifier activation information;
receiving, from a management node, the user identifier and an activation result of the user identifier;
forwarding, from an application node or a network exposure node to a management node, a first message for activating the user identifier; or
forwarding, from a management node to an application node or a network exposure node, a second message comprising the user identifier and an activation result of the user identifier.
8. The wireless communication method of claim 7, wherein the anchor node acquires the user identifier activation information based on a key identifier received from an application node.
9. The wireless communication method of any of claims 1 to 8, wherein the wireless communication node comprises an application node, and the application node performs

at least one of:

transmitting, to a management node, a first message for activating the user identifier; or
transmitting, to a management node, a third message indicating whether the user identifier is successfully activated.

10. The wireless communication method of claim 9, wherein the application node transmits the first or third message in response to a decrypted user identifier matches user identifier activation information from an anchor node.
11. The wireless communication method of claim 10, wherein the application node checks whether the decrypted user identifier matches the user identifier activation information based on a service type from the request message.
12. The wireless communication method of any of claims 8 to 11, wherein the application node decrypts the request message to acquire a decrypted user identifier and/or a service type.
13. The wireless communication method of any of claims 1 to 12, wherein the request message comprises a User Identities and Authentication, UIA, Active Request message received by a management node of the wireless communication node and/or an Application Session Establishment Request message received by an application node of the wireless communication node; and/or
wherein the response message comprises a UIA Active Response message transmitted from a management node of the wireless communication node to the wireless communication terminal and/or an Application Session Establishment Response message transmitted from an application node of the wireless communication node to the wireless communication terminal.
14. A wireless communication method comprising:
transmitting, by a wireless communication terminal to a wireless communication node,

a request message comprising a user identifier to be activated; and
receiving, by the wireless communication terminal from the wireless communication node, a response message indicating whether the user identifier is successfully activated or whether a session for the user identifier is established.

15. The wireless communication method of claim 14, wherein a first response message of the request message transmitted to a management node of the wireless communication node comprises the user identifier and an activation result of the user identifier.
16. The wireless communication method of claim 14 or 15, wherein a first request message of the request message transmitted to a management node of the wireless communication node comprises a User Identities and Authentication, UIA, Active Request message and/or a first response message of the response message received from a management node of the wireless communication node comprises a UIA Active Response message.
17. The wireless communication method of any of claims 14 to 16, wherein a second request message of the request message transmitted to an application node of the wireless communication node further comprises a service type for activating the user identifier.
18. The wireless communication method of claim 17, wherein the user identifier and/or the service type in the second request message is encrypted.
19. The wireless communication method of any of claims 14 to 18, wherein a second request message of the request message transmitted to an application node of the wireless communication node comprises an Application Session Establishment Request message and/or a second response message of the response message received from an application node of the wireless communication node comprises an Application Session Establishment Response message.

20. A wireless communication terminal, comprising:
a communication unit; and
a processor configured for: receiving, via the communication unit from a wireless communication terminal, a request message comprising a user identifier to be activated; and transmitting, by the wireless communication node to the wireless communication terminal, a response message indicating whether the user identifier is successfully activated or whether a session for the user identifier is established.
21. The wireless communication terminal of claim 20, wherein the processor is further configured to perform a wireless communication method of any of claims 2 to 13.
22. A wireless communication node, comprising:
a communication unit; and
a processor configured to: transmitting, via the communication unit to a wireless communication node, a request message comprising a user identifier to be activated; and receiving, by the wireless communication terminal from the wireless communication node, a response message indicating whether the user identifier is successfully activated or whether a session for the user identifier is established.
23. The wireless communication node of claim 22, wherein the processor is further configured to perform a wireless communication method of any of claims 15 to 19.
24. A computer program product comprising a computer-readable program medium code stored thereupon, the code, when executed by a processor, causing the processor to implement a wireless communication method recited in any one of claims 1 to 19.

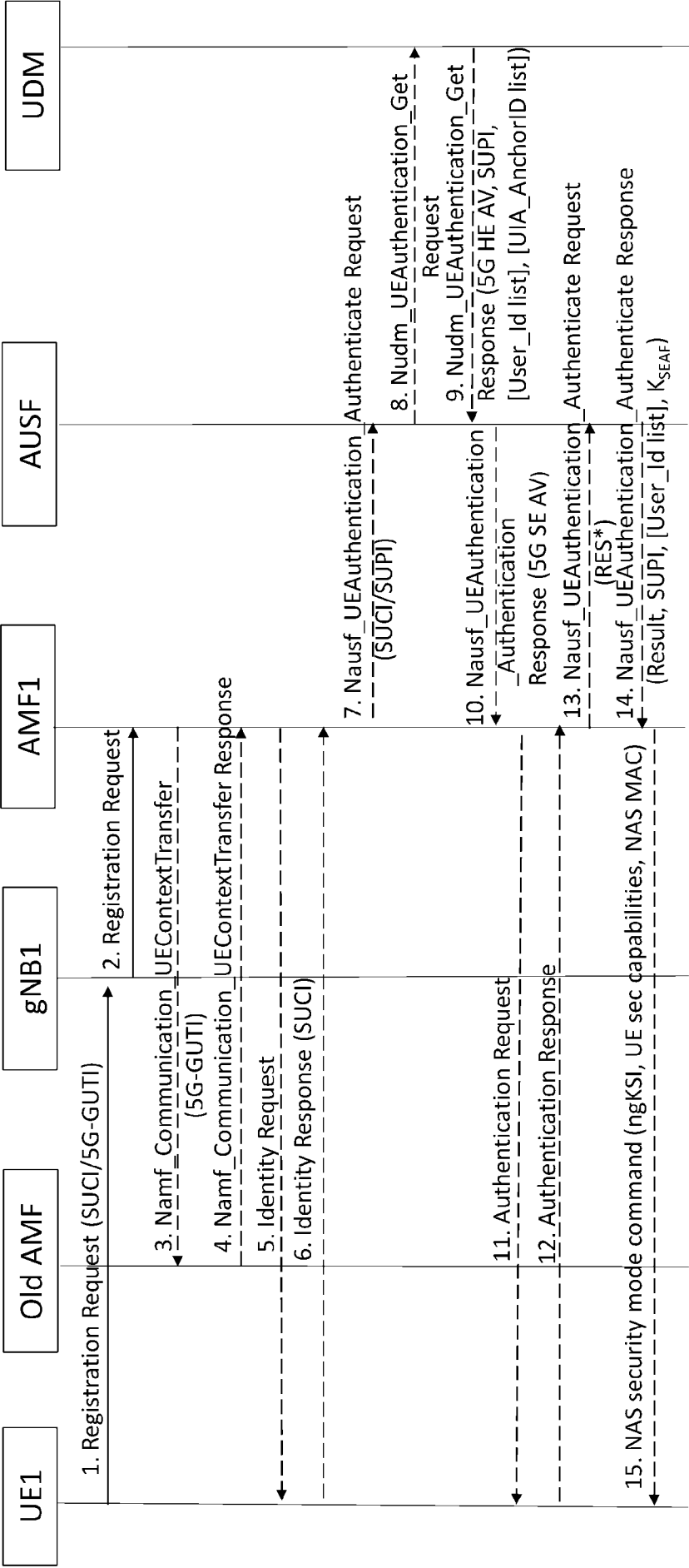


FIG. 1A

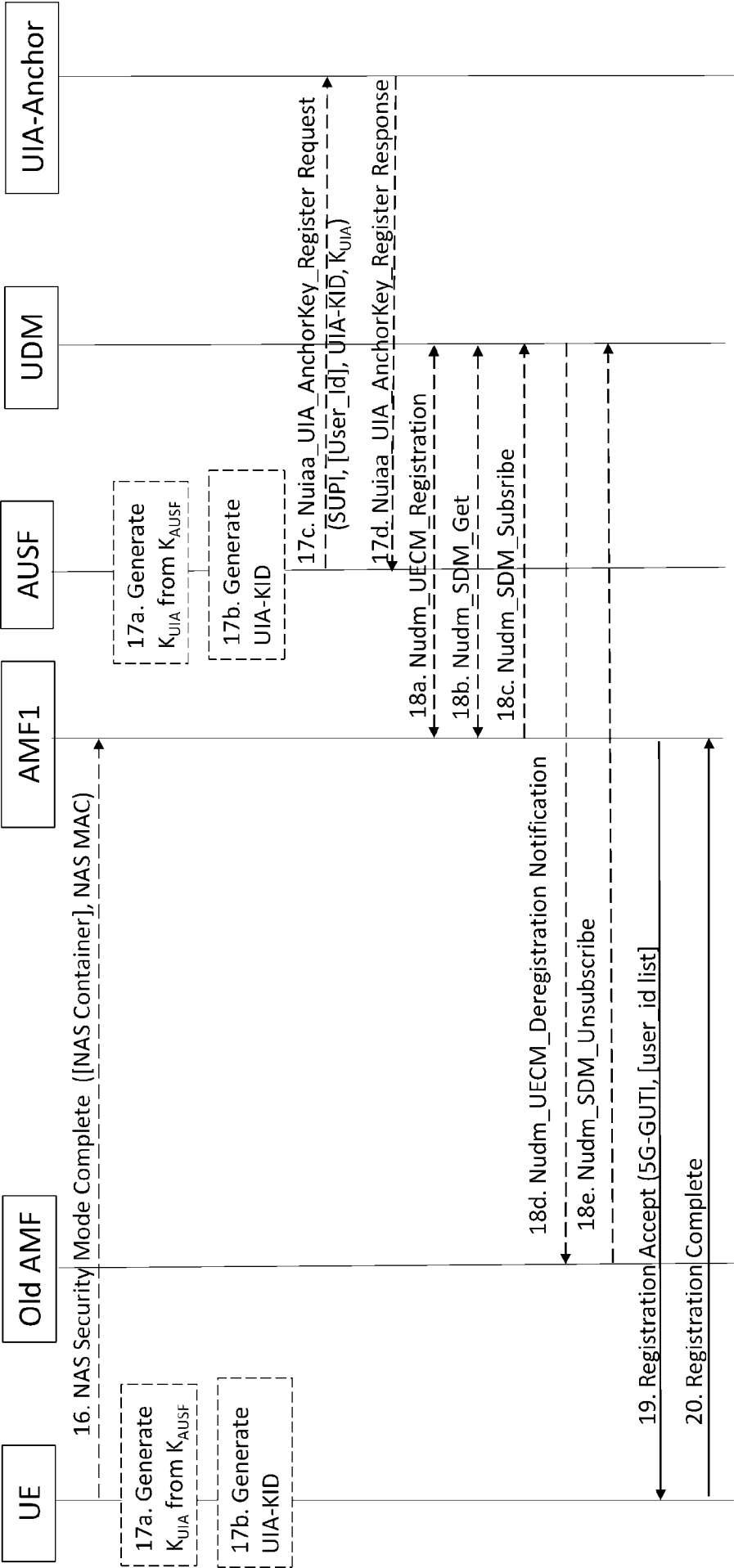


FIG. 1B

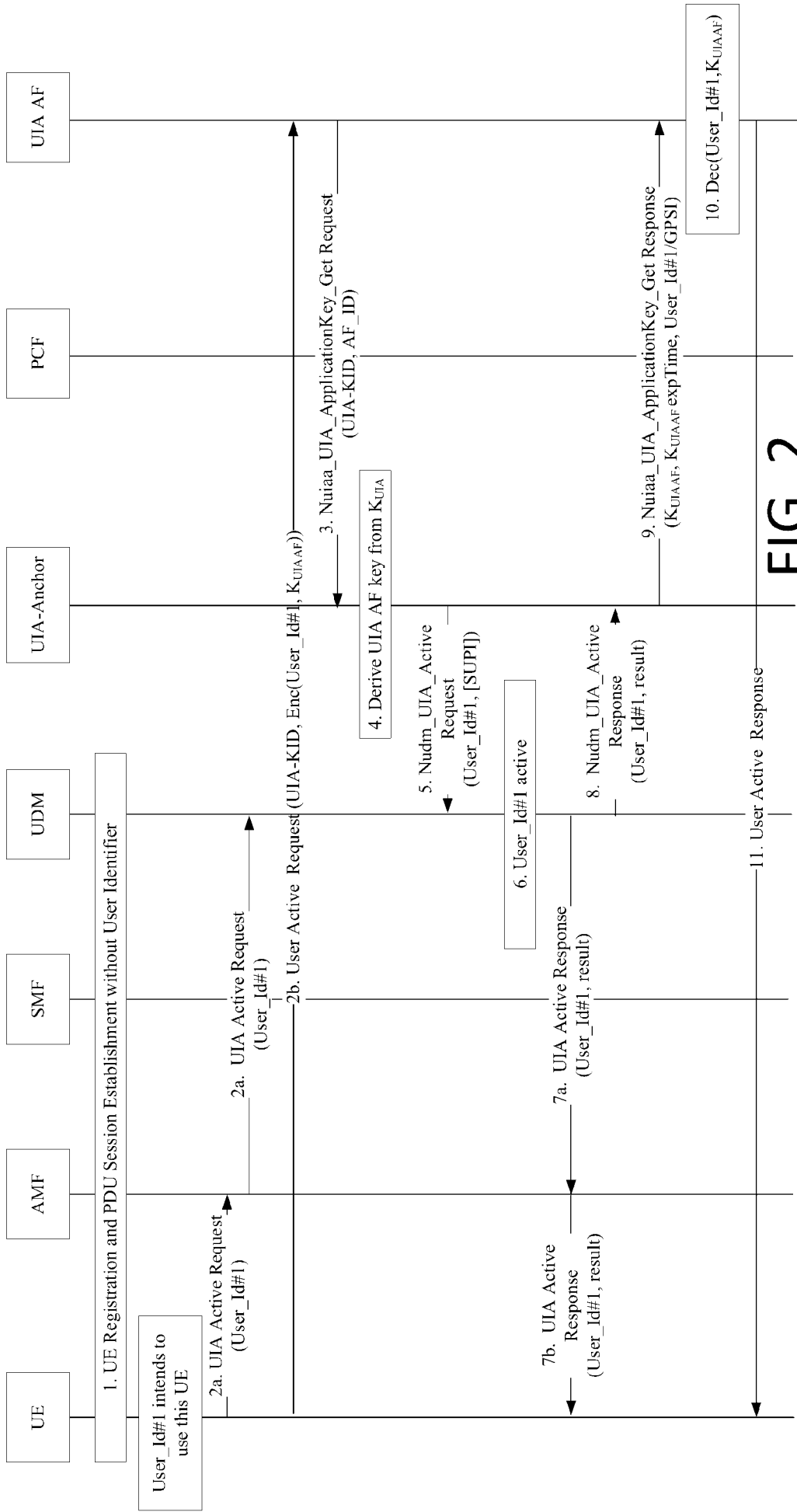


FIG. 2

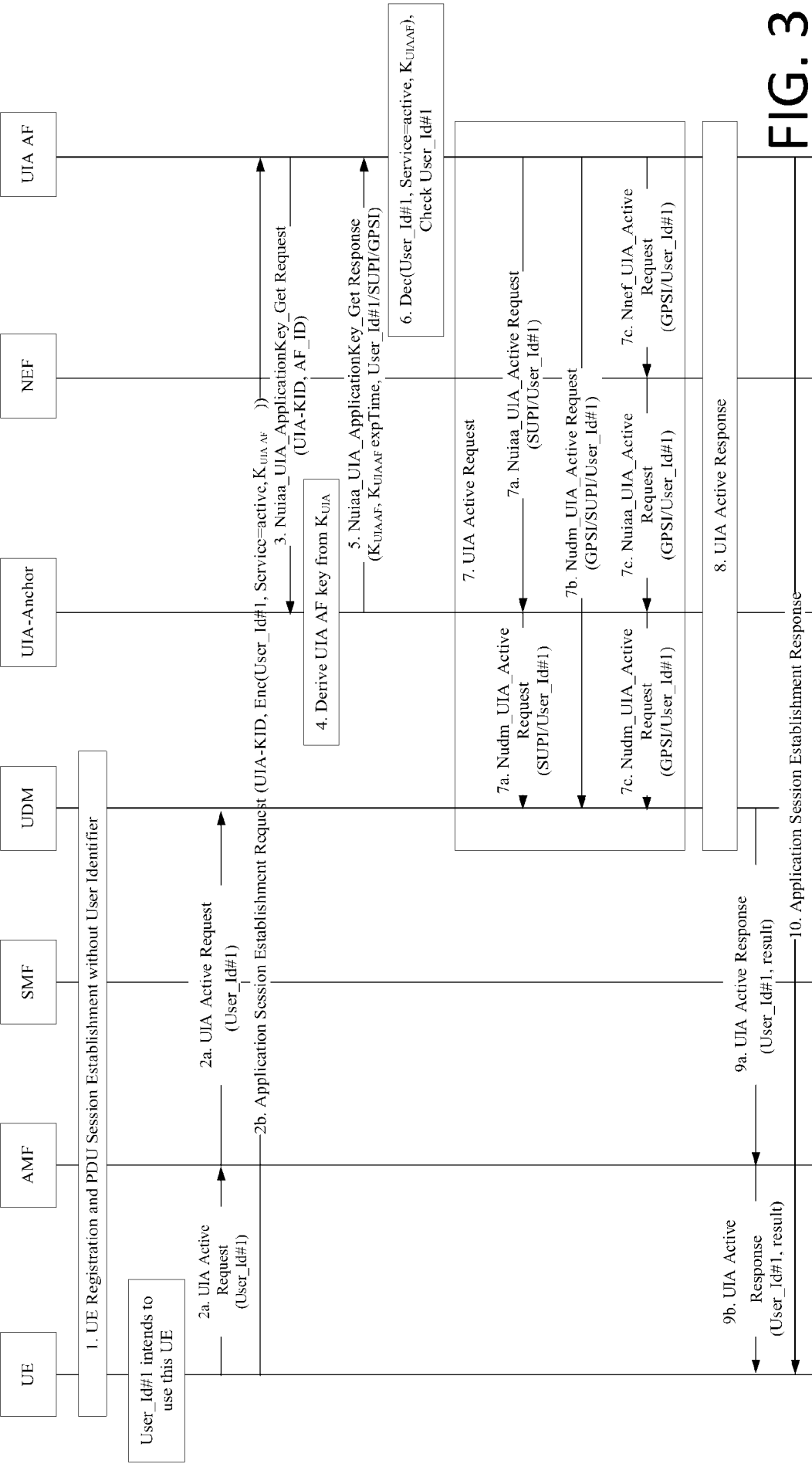


FIG. 3

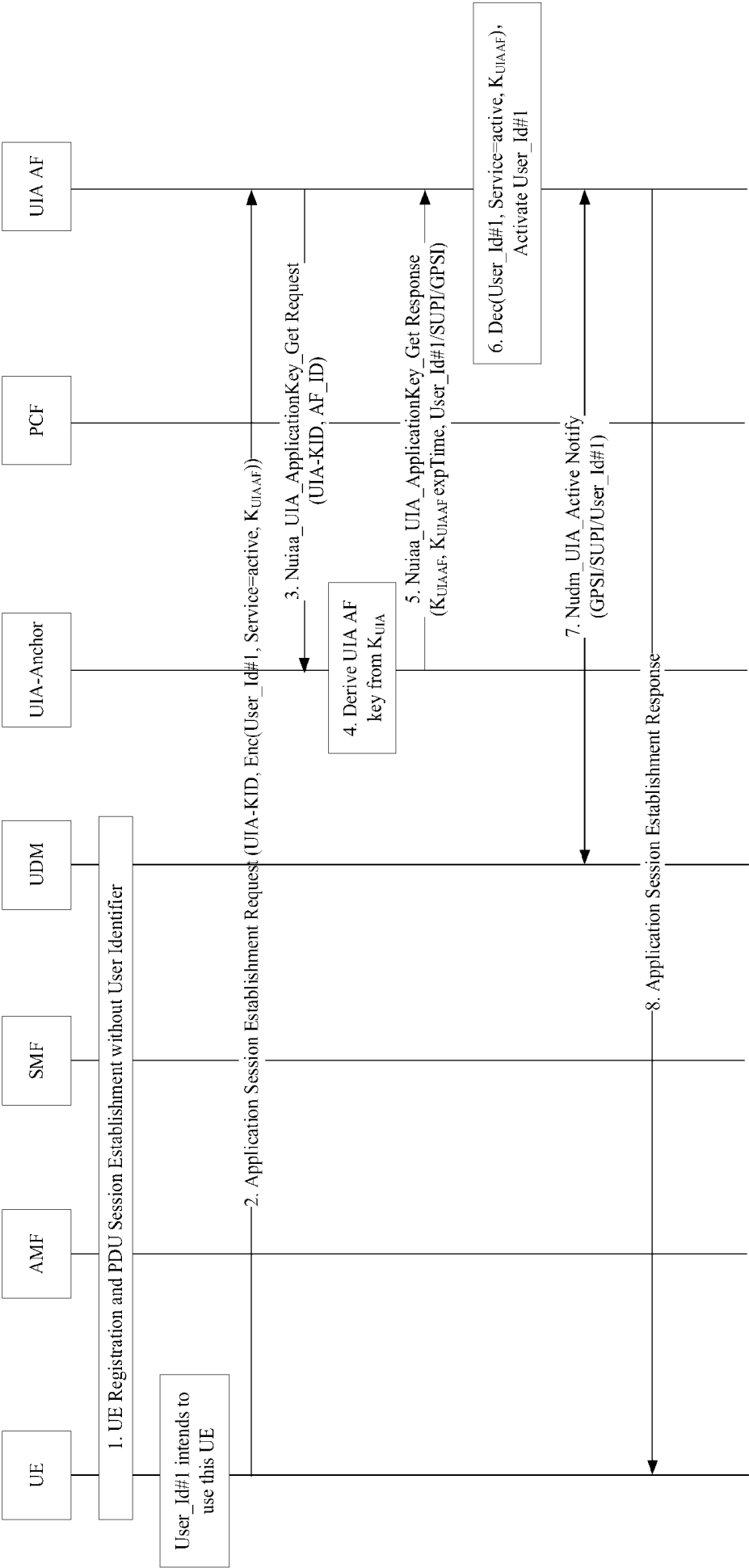


FIG. 4

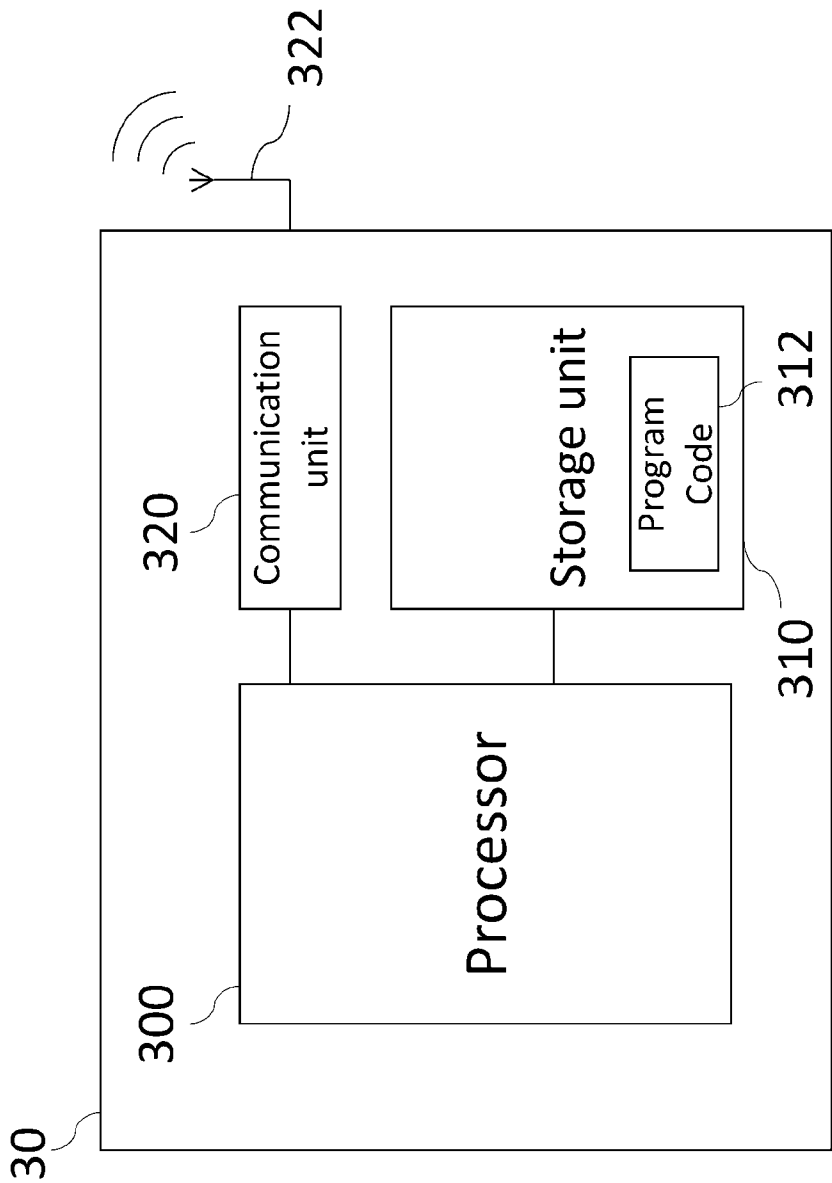


FIG. 5

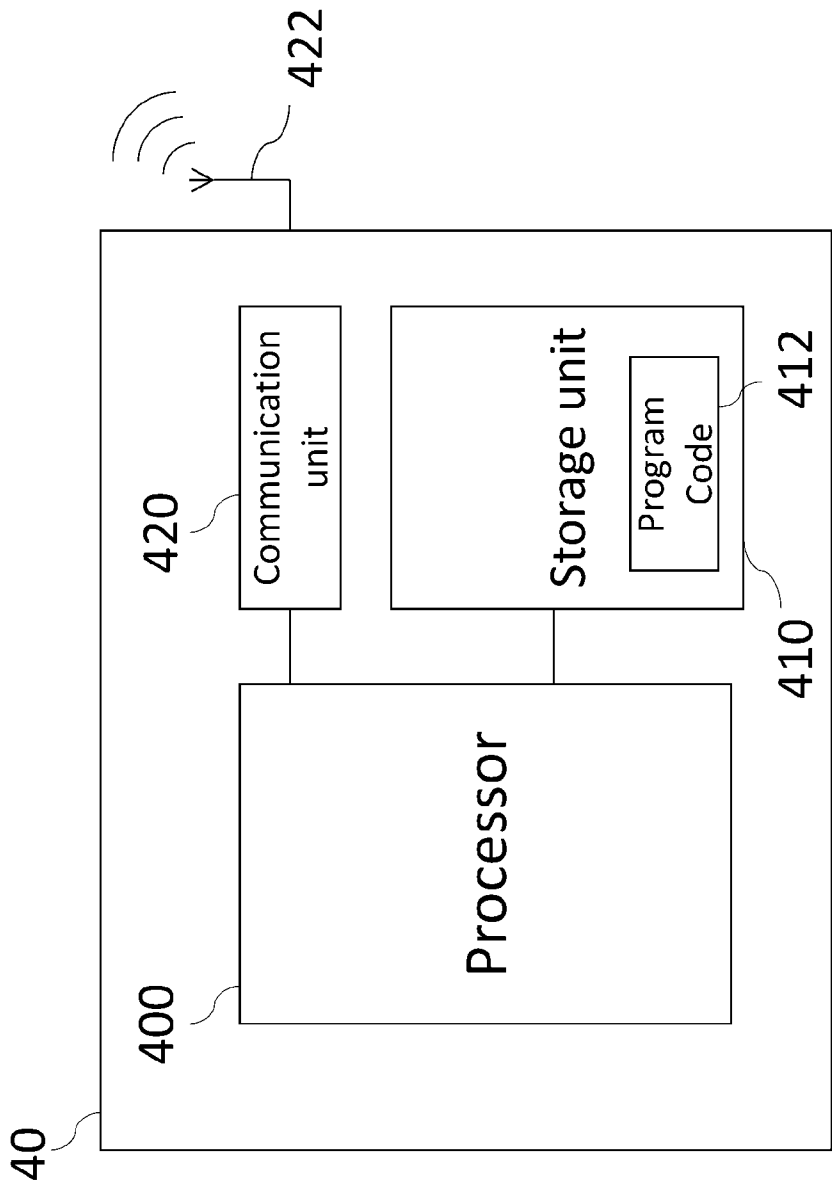


FIG. 6

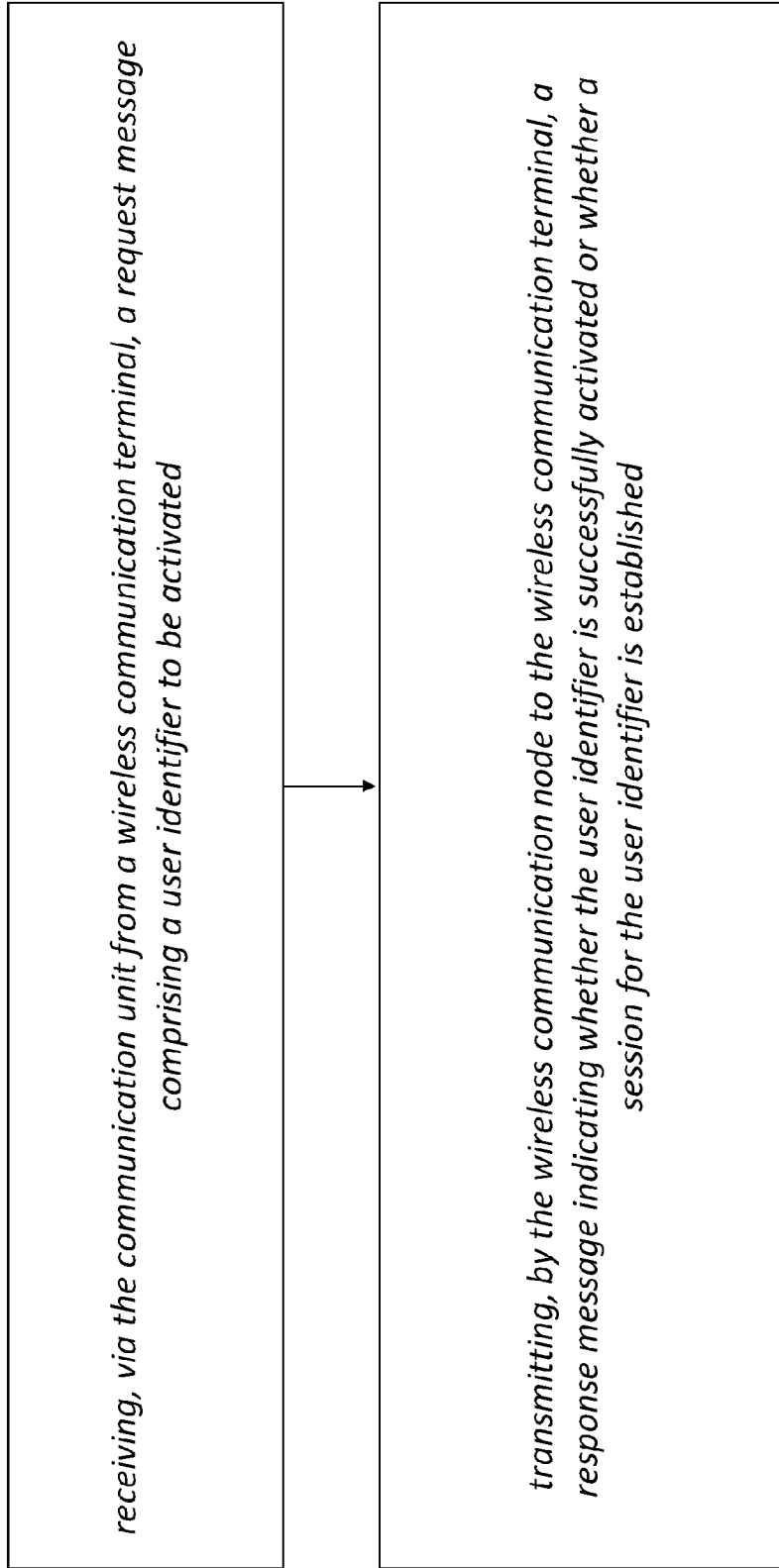


FIG. 7

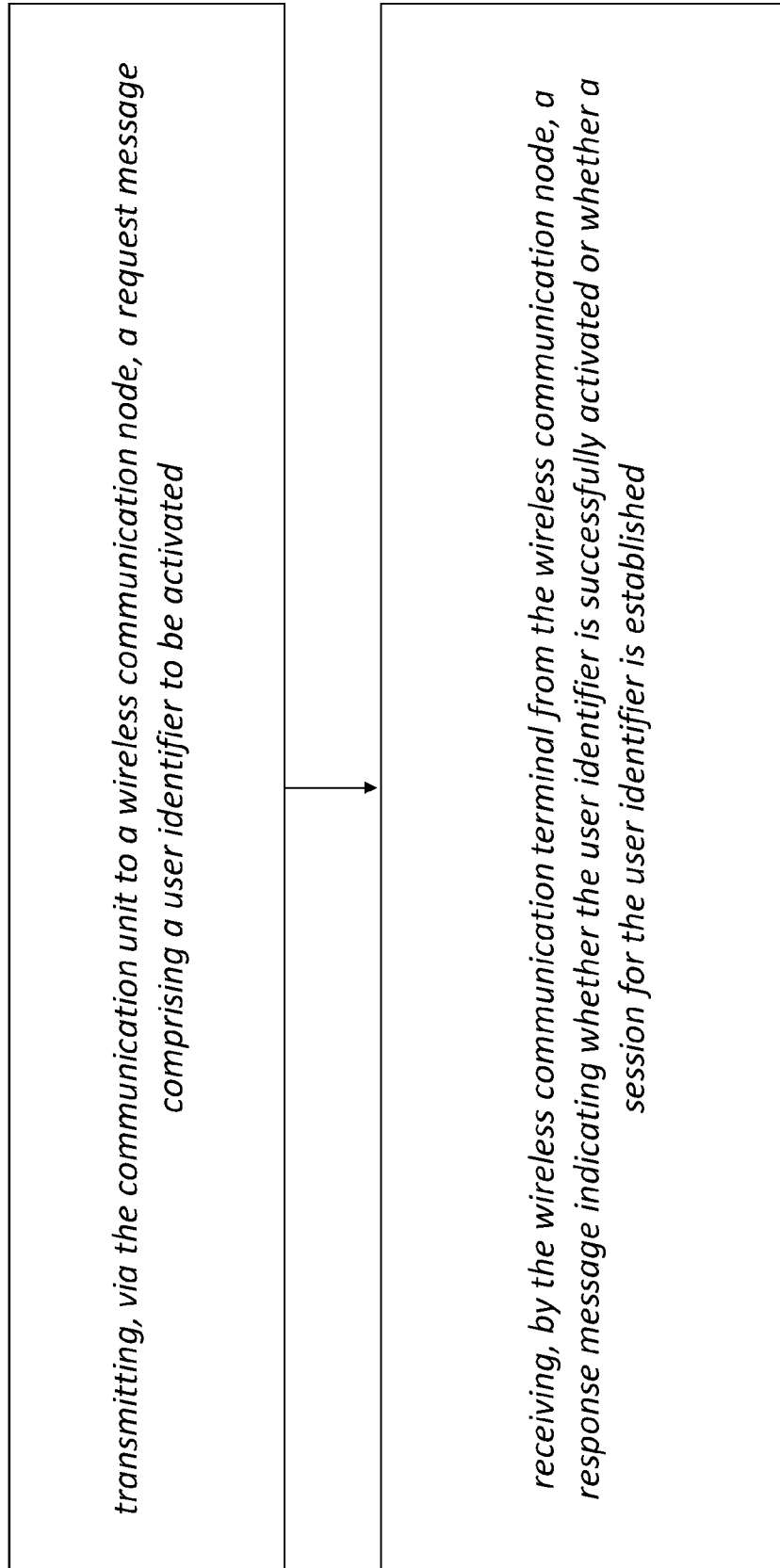


FIG. 8

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2024/111114

A. CLASSIFICATION OF SUBJECT MATTER H04W12/08(2021.01)i According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED Minimum documentation searched (classification system followed by classification symbols) IPC: H04W Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched Electronic data base consulted during the international search (name of data base and, where practicable, search terms used) 3GPP,ENTXT,CNXT,DWPI:user, ID, identifier, UIA, activate, active, authentication, anchor, request, response, human, SUPI, SUCI, GPSI		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	3GPP TSG SA. "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Study on security aspects of User Identities and Authentication (Release 19)" 3GPP TR 33.700-32 V0.2.0, 30 May 2024 (2024-05-30), clauses 6.4.2.2, 6.8.2.2	1,13-14,17-24
X	3GPP TSG SA. "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Study on User Identities and Authentication Architecture (Release 19)" 3GPP TR 23.700-32 V1.0.0, 10 June 2024 (2024-06-10), clauses 6.3.3.2, 6.17.3.2	1,13-14,17-24
X	ZTE CORPORATION. "Solution to KI#1 and KI#2" 3GPP TSG-SA3 Meeting #116 S3-242499, 24 May 2024 (2024-05-24), clause 6.Y.2.2	1,13-14,17-24
X	CN 114503630 A (SAMSUNG ELECTRONICS CO., LTD.) 13 May 2022 (2022-05-13) description, paragraphs 85-128	1,14,20,22,24
☒ 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 21 April 2025		Date of mailing of the international search report 24 April 2025
Name and mailing address of the ISA/CN CHINA NATIONAL INTELLECTUAL PROPERTY ADMINISTRATION 6, Xitucheng Rd., Jimen Bridge, Haidian District, Beijing 100088, China		Authorized officer YAN,Yan Telephone No. (+86) 010-53961631

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2024/111114

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	ZTE. "KI#1, conclusion update" SA WG2 Meeting #S2-163 S2-2406616, 31 May 2024 (2024-05-31), the whole document	1-24
A	US 2022264504 A1 (NEC CORPORATION) 18 August 2022 (2022-08-18) the whole document	1-24

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2024/111114

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	114503630	A	13 May 2022	WO	2021066452	A1	08 April 2021
				EP	4247115	A2	20 September 2023
				US	2022338000	A1	20 October 2022
				EP	4007326	A1	01 June 2022
US	2022264504	A1	18 August 2022	JP	2022538658	A	05 September 2022
				WO	2021002274	A1	07 January 2021
				EP	3994907	A1	11 May 2022