



- (51) **International Patent Classification:**
H04W 12/06 (2009.01) *H04W 88/06* (2009.01)
H04W 36/14 (2009.01) *H04W 92/02* (2009.01)
- (21) **International Application Number:**
PCT/SE2014/051454
- (22) **International Filing Date:**
4 December 2014 (04.12.2014)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
62/013,640 18 June 2014 (18.06.2014) US
- (71) **Applicant:** TELEFONAKTIEBOLAGET L M ERICSSON (PUBL) [SE/SE]; SE-164 83 Stockholm (SE).
- (72) **Inventors:** NILSSON, Daniel; Båtsmansvägen 34, S-446 33 Älvängen (SE). CHEN, Qian; Eklanda Skog 64, S-431 49 Mölndal (SE). WANG, Chunbo; 302#, No.25, Lane 99, Jinhe Road, Pudong New Area, Shanghai 200127 (CN).
- (74) **Agent:** AYOUB, Nabil; Ericsson AB, Patent Unit Kista RAN2, SE-16480 Stockholm (SE).
- (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, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, 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, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

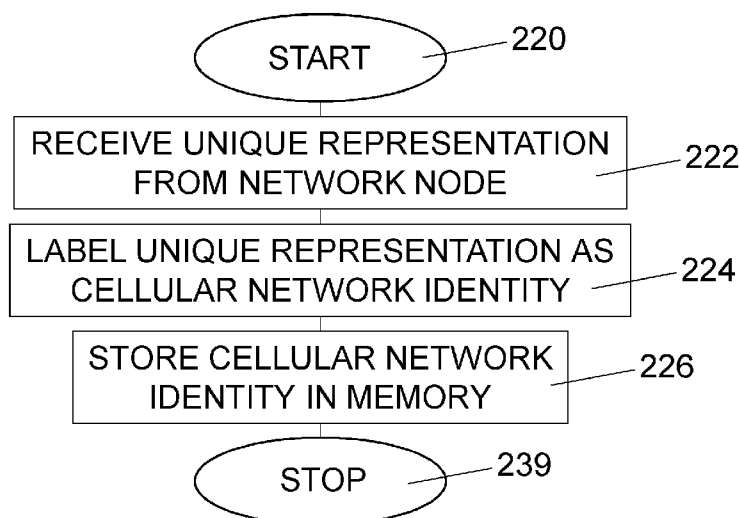
- (84) **Designated States** (*unless otherwise indicated, for every kind of regional protection available*): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, 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).

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))

(54) **Title:** METHODS AND ARRANGEMENTS FOR IDENTIFICATION OF USER EQUIPMENTS FOR AUTHENTICATION PURPOSES

FIG 5



(57) **Abstract:** A method for assigning a cellular network identity. The method comprises receiving(222), in a user equipment capable to attach to a cellular network and a wireless local area network, a unique representation of a user equipment context of the user equipment and in what cellular network node the user equipment is or is going to be attached, from a network node. The unique representation is labelled (224) as a cellular network identity and cellular network identity is stored (226) a pseudonym identity and/or a fast re-authentication identity in a memory in the user equipment.



METHODS AND ARRANGEMENTS FOR IDENTIFICATION OF USER EQUIPMENTS FOR AUTHENTICATION PURPOSES

TECHNICAL FIELD

5

The proposed technology generally relates to attachment of user equipment to cellular networks and wireless local area networks, and in particular to the process of authentication.

10

BACKGROUND

Mobile operators are today mainly using Wi-Fi to offload traffic from the mobile networks but the opportunity to improve end user experience regarding performance is also becoming more important. The current Wi-Fi
15 deployments are mainly totally separate from mobile networks, and are to be seen as non-integrated. The usage of Wi-Fi is mainly driven due to the free and wide unlicensed spectrum, and the increased availability of Wi-Fi in mobile terminals like smartphones and tablets. The end users are also becoming more and more at ease with using Wi-Fi for example at offices and
20 homes.

The different business segments for Wi-Fi regarding integration possibilities can be divided into mobile operator hosted/controlled vs. 3rd party hosted/controlled Wi-Fi Access Points (Aps) (here 3rd party is seen as
25 anything else than mobile operator and that the 3rd party is not totally "trusted" by the mobile operator. 3rd party could be for example a Wi-Fi operator or an end-user him/herself.). In both segments there exist public/hotspot, enterprise and residential deployments.

30 Wi-Fi integration towards the mobile core network is emerging as a good way to improve the end user experience further. These solutions consist mainly of the components: common authentication between 3GPP (3rd Generation Partnership Project) and Wi-Fi, and integration of Wi-Fi user

plane traffic to the mobile core network. The common authentication is based on automatic Subscriber Identity Module (SIM) based authentication in both access types. The Wi-Fi user plane integration provides the mobile operator the opportunity to provide the same services, like parental control
5 and subscription based payment methods, for the end users when connected both via 3GPP and via Wi-Fi. Different solutions are standardized in 3GPP: Overlay solutions (S2b, S2c) are specified since 3GPP Rel-8 while integration solutions (S2a) are currently work-in-progress (S2a, S2b, S2c indicating the 3GPP interface/reference point name towards the PDN-
10 gateway (GW)). These solutions are specified in 3GPP TS 23.402.

Most solutions of today require extensive signaling to a common authentication node, requiring resources and being a potential security risk.

15

SUMMARY

It is an object to provide methods and arrangements providing a more coordinated authentication process between wireless local area networks and cellular networks.

20

This and other objects are met by embodiments of the proposed technology.

According to a first aspect, there is provided a method for assigning a cellular network identity. The method comprises identifying, by a network node of a
25 communication network as a response to an attach message from a user equipment, a user equipment context of the user equipment and in what cellular network node the user equipment is or is going to be attached. A unique representation of the identified user equipment context and the cellular network node is generated. The unique representation is labelled as
30 a cellular network identity, wherein the cellular network identity is a pseudonym identity or a fast re-authentication identity. The unique representation is sent to the user equipment as the pseudonym identity or the fast re-authentication identity.

According to a second aspect, there is provided a method for assigning a cellular network identity. The method comprises receiving, in a user equipment capable to attach to a cellular network and a wireless local area network, a unique representation of a user equipment context of the user
5 equipment and in what cellular network node the user equipment is or is going to be attached, from a network node. The unique representation is labelled as a cellular network identity and the cellular network identity is stored as a pseudonym identity and/or a fast re-authentication identity in a memory in the user equipment.

10

According to a third aspect, there is provided a method for identifying a user equipment upon attaching the user equipment to a wireless communication network. The method comprises retrieving, from a memory in the user equipment, a unique representation of a user equipment context of the user
15 equipment and in what cellular network node the user equipment is or is going to be attached. The unique representation is labelled as a cellular network identity, wherein the cellular network identity is a pseudonym identity or a fast re-authentication identity. A cellular network identity comprising the unique representation as a user identity is sent in an attach
20 procedure to the wireless communication network.

According to a fourth aspect, there is provided a method for assisting in attaching a user equipment to a wireless communication network. The method comprises receiving, in a network node, of a user identity from a
25 user equipment. The method further comprises a determination of whether or not the received user identity is a cellular network identity, wherein the cellular network identity is a pseudonym identity or a fast re-authentication identity comprising a unique representation of a user equipment context of the user equipment and in what cellular network node the user equipment
30 is or is going to be attached. If it is determined that the received user identity is a cellular network identity, an authentication procedure is directed towards an authentication node defined by the cellular network identity.

According to a fifth aspect, there is provided a network node of a communication network. The network node comprises an input, a processor, a memory and an output. The memory comprising instructions executable by the processor whereby the network node is operative to
5 identify, as a response to an attach message from a user equipment, a user equipment context of the user equipment and in what cellular network node the user equipment is or is going to be attached. The memory comprises further instructions executable by the processor whereby the network node is operative to generate a unique representation of the identified user
10 equipment context and the cellular network node. The memory comprises further instructions executable by the processor whereby the network node is operative to label the unique representation as a cellular network identity, wherein the cellular network identity is a pseudonym identity or a fast re-authentication identity. The memory comprises further instructions
15 executable by the processor whereby the network node is operative to send the unique representation as the pseudonym identity or the fast re-authentication identity via the output to the user equipment.

According to a sixth aspect, there is provided a network node of a
20 communication network. The network node comprises an input, a processor, a memory and an output. The memory comprising instructions executable by the processor whereby the network node is operative to receive a user identity from a user equipment via the input. The memory comprises further instructions executable by the processor whereby the
25 network node is operative to determine whether or not the received user identity is a cellular network identity, wherein the cellular network identity is a pseudonym identity or a fast re-authentication identity comprising a unique representation of a user equipment context of the user equipment and in what cellular network node the user equipment is or is going to be
30 attached. The memory comprises further instructions executable by the processor whereby the network node is operative to direct, if determined that the received user identity is a cellular network identity, an authentication procedure towards an authentication node defined by the cellular network identity.

According to a seventh aspect, there is provided a user equipment capable to attach to a cellular network and a wireless local area network. The user equipment comprises an input, a processor and a memory. The memory
5 comprises instructions executable by the processor whereby the user equipment is operative to receive, from a network node via the input, a unique representation of a user equipment context of the user equipment and in what cellular network node the user equipment is or is going to be attached. The memory comprises further instructions executable by the
10 processor whereby the user equipment is operative to label the unique representation as a cellular network identity. The memory comprises further instructions executable by the processor whereby the user equipment is operative to store the cellular network identity as a pseudonym identity and/or a fast re-authentication identity in the memory.

15

According to an eighth aspect, there is provided a user equipment capable to attach to a cellular network and a wireless local area network. The user equipment comprises a processor, a memory and an output. The memory comprises instructions executable by the processor whereby the user
20 equipment is operative to retrieve, from the memory, a unique representation of a user equipment context of the equipment and in what cellular network node the user equipment is or is going to be attached. The memory comprises further instructions executable by the processor whereby the user equipment is operative to label the unique representation as a
25 cellular network identity, wherein the cellular network identity is a pseudonym identity or a fast re-authentication identity, and to send, via the output, a cellular network identity comprising the unique representation as a user identity in an attach procedure to the wireless communication network.

30

According to a ninth aspect, there is provided a network node in a wireless communication network. The network node comprises an identifying module for identifying, as a response to an attach message from a user equipment, a user equipment context of the user equipment and in what cellular network

node the user equipment is or is going to be attached. The network node further comprises a generating module for generating a unique representation of the identified user equipment context and the cellular network node. The network node further comprises a labelling module for
5 labelling the unique representation as a cellular network identity, wherein the cellular network identity is a pseudonym identity or a fast re-authentication identity. The network node further comprises a sending module for sending the unique representation to the user equipment as the pseudonym identity or the fast re-authentication identity.

10

According to a tenth aspect, there is provided a user equipment capable to attach to a cellular network and a wireless local area network. The user equipment comprises a receiving module for receiving a unique representation of a user equipment context of the user equipment and in
15 what cellular network node the user equipment is or is going to be attached, from a network node. The user equipment further comprises a labelling module for labelling the unique representation as a cellular network identity. The user equipment further comprises a memory. The user equipment further comprises a storing module for storing the cellular
20 network identity as a pseudonym identity and/or a fast re-authentication identity in the memory.

According to an eleventh aspect, there is provided a user equipment capable to attach to a cellular network and a wireless local area network. The user
25 equipment comprises a memory. The user equipment further comprises a retrieving module for retrieving, from the memory, a unique representation of a user equipment context of the user equipment and in what cellular network node the user equipment is or is going to be attached. The user equipment further comprises a labelling module for labelling the unique
30 representation as a cellular network identity, wherein the cellular network identity is a pseudonym identity or a fast re-authentication identity. The user equipment further comprises a sending module for sending a cellular network identity comprising the unique representation as a user identity in an attach procedure to the wireless communication network.

According to a twelfth aspect, there is provided a network node in a wireless communication network. The network node comprises a receiving module for receiving a user identity from a user equipment. The network node
5 further comprises a determining module for determining whether or not the received user identity is a cellular network identity, wherein the cellular network identity is a pseudonym identity or a fast re-authentication identity comprising a unique representation of a user equipment context of the user equipment and in what cellular network node the user equipment is or is
10 going to be attached. The network node further comprises a directing module for directing, if determined that the received user identity is a cellular network identity, an authentication procedure towards an authentication node defined by the cellular network identity.

15 According to a thirteenth aspect, there is provided a computer program, residing in a memory. The computer program comprises program code, which when executed by a processing circuitry causes the processing circuitry to identify, as a response to an attach message from a user equipment, a user equipment context of the user equipment and in what
20 cellular network node the user equipment is or is going to be attached. The computer program further comprises program code, which when executed by the processing circuitry causes the processing circuitry to generate a unique representation of the identified user equipment context and the cellular network node. The computer program further comprises program
25 code, which when executed by the processing circuitry causes the processing circuitry to label the unique representation as a cellular network identity, wherein the cellular network identity is a pseudonym identity and/or a fast re-authentication identity. The computer program further comprises program code, which when executed by the processing circuitry
30 causes the processing circuitry to send the unique representation via an output to the user equipment as the pseudonym identity or the fast re-authentication identity.

According to a thirteenth aspect, there is provided a computer program, residing in a memory. The computer program comprises program code, which when executed by a processing circuitry causes the processing circuitry to receive, from a network node via an input, a unique
5 representation of a user equipment context of the user equipment and in what cellular network node the user equipment is or is going to be attached. The computer program further comprises program code, which when executed by the processing circuitry causes the processing circuitry to label the unique representation as a cellular network identity. The computer
10 program further comprises program code, which when executed by the processing circuitry causes the processing circuitry to store the cellular network identity as a pseudonym identity and/or a fast re-authentication identity in the memory.

15 According to a fourteenth aspect, there is provided a computer program, residing in a memory. The computer program comprises program code, which when executed by a processing circuitry causes the processing circuitry to retrieve, from the memory, a unique representation of a user equipment context of the user equipment and in what cellular network node
20 the user equipment is or is going to be attached. The computer program further comprises program code, which when executed by the processing circuitry causes the processing circuitry to label the unique representation as a cellular network identity, wherein the cellular network identity is a pseudonym identity or a fast re-authentication identity. The computer
25 program further comprises program code, which when executed by the processing circuitry causes the processing circuitry to send, via an output, a cellular network identity comprising the unique representation as a user identity in an attach procedure to the wireless communication network.

30 According to a fifteenth aspect, there is provided a computer program, residing in a memory. The computer program comprises program code, which when executed by a processing circuitry causes the processing circuitry to identify, as a response to an attach message from a user equipment, a user equipment context of the user equipment and in what

cellular network node the user equipment is or is going to be attached. The computer program further comprises program code, which when executed by the processing circuitry causes the processing circuitry to generate a unique representation of the identified user equipment context and the
5 cellular network node. The computer program further comprises program code, which when executed by the processing circuitry causes the processing circuitry to label the unique representation as a cellular network identity, wherein the cellular network identity is a pseudonym identity and/or a fast re-authentication identity. The computer program further
10 comprises program code, which when executed by the processing circuitry causes the processing circuitry to send the unique representation via an output to the user equipment.

According to a sixteenth aspect, there is provided a computer program,
15 residing in a memory. The computer program comprises program code, which when executed by a processing circuitry causes the processing circuitry to receive a user identity from a user equipment via an input. The computer program further comprises program code, which when executed by the processing circuitry causes the processing circuitry to determine
20 whether or not the received user identity is a cellular network identity, wherein the cellular network identity is a pseudonym identity or a fast re-authentication identity comprising a unique representation of a user equipment context of the user equipment and in what cellular network node the user equipment is or is going to be attached. The computer program
25 further comprises program code, which when executed by the processing circuitry causes the processing circuitry to direct, if determined that the received user identity is a cellular network identity, an authentication procedure towards an authentication node defined by the cellular network identity.

30

According to a seventeenth aspect, there is provided a computer program product. The computer program comprises program code, which when executed by a processing circuitry causes the processing circuitry to identify, as a response to an attach message from a user equipment, a user

equipment context of the user equipment and in what cellular network node the user equipment is or is going to be attached. The computer program further comprises program code, which when executed by a processing circuitry causes the processing circuitry to generate a unique representation
5 of the identified user equipment context and the cellular network node. The computer program further comprises program code, which when executed by a processing circuitry causes the processing circuitry to label the unique representation as a cellular network identity, wherein the cellular network identity is a pseudonym identity or a fast re-authentication identity. The
10 computer program further comprises program code, which when executed by a processing circuitry causes the processing circuitry to send the unique representation as the pseudonym identity or the fast re-authentication identity via an output to the user equipment.

15 According to an eighteenth aspect, there is provided a computer program product comprising a computer-readable medium on which a computer program is stored. The computer program comprises program code, which when executed by a processing circuitry causes the processing circuitry to receive, from a network node via an input, a unique representation of a user
20 equipment context of the user equipment and in what cellular network node the user equipment is or is going to be attached. The computer program further comprises program code, which when executed by a processing circuitry causes the processing circuitry to label the unique representation as a cellular network identity. The computer program further comprises
25 program code, which when executed by a processing circuitry causes the processing circuitry to store the cellular network identity as a pseudonym identity and/or a fast re-authentication identity in a memory.

According to a nineteenth aspect, there is provided a computer program
30 product comprising a computer-readable medium on which a computer program is stored. The computer program comprises program code, which when executed by a processing circuitry causes the processing circuitry to retrieve, from a memory, a unique representation of a user equipment context of the user equipment and in what cellular network node the user

equipment is or is going to be attached. The computer program further comprises program code, which when executed by a processing circuitry causes the processing circuitry to label the unique representation as a cellular network identity, wherein the cellular network identity is a
5 pseudonym identity or a fast re-authentication identity. The computer program further comprises program code, which when executed by a processing circuitry causes the processing circuitry to send, via an output, a cellular network identity comprising the unique representation as a user identity in an attach procedure to the wireless communication network.

10

According to a twentieth aspect, there is provided a computer program product comprising a computer-readable medium on which a computer program is stored. The computer program comprises program code, which when executed by a processing circuitry causes the processing circuitry to
15 receive a user identity from a user equipment via an input. The computer program further comprises program code, which when executed by a processing circuitry causes the processing circuitry to determine whether or not the received user identity is a cellular network identity, wherein the cellular network identity is a pseudonym identity or a fast re-authentication
20 identity comprising a unique representation of a user equipment context of the user equipment and in what cellular network node the user equipment is or is going to be attached. The computer program further comprises program code, which when executed by a processing circuitry causes the processing circuitry to direct, if determined that the received user identity is
25 a cellular network identity, an authentication procedure towards an authentication node defined by the cellular network identity.

Embodiments of the proposed technology enables/makes it possible to coordinate features between cellular network and non-cellular network
30 access, e.g. 3GPP and non-3GPP access (e.g. WiFi access).

The solution will work with minimal to none standard changes meaning that this solution can be launched in a product quite easily. There might still be some UE impact.

Additionally there is no need with the proposed technology to introduce new databases to map users between the accesses.

5 Lastly, because it is e.g. the SGSN/MME (Serving General packet radio services Support Node/Mobility Management Entity) identity that is stored in the UE 3GPP identity, the 3GPP identity can be semi-static and only have to be changed in the case when UE is move from one SGSN/MME to another which is done quite seldom

10

Other advantages will be appreciated when reading the detailed description.

BRIEF DESCRIPTION OF THE DRAWINGS

15 The embodiments, together with further objects and advantages thereof, may best be understood by making reference to the following description taken together with the accompanying drawings, in which:

FIG. 1A is an illustration of the existing network architectures for Evolved
20 Universal Terrestrial Radio Access Network/ Evolved Packet Core (E-UTRAN/EPC) and S2a integration;

FIG. 1B is an illustration of a typical deployment for untrusted WiFi access;

FIG. 2 illustrates a process flow of Wireless Local Area Network (WLAN)
Retransmission Sequence Number (RSN) authentication (with EAP-
25 SIM);

FIG. 3 illustrates how SGSN/MME may do authentication for both trusted and untrusted WiFi access;

FIG. 4 illustrates a flow diagram of steps of an embodiment of a method in a network node for assigning a cellular network identity;

30 FIG. 5 illustrates a flow diagram of steps of an embodiment of a method in a user equipment for assigning a cellular network identity;

FIG. 6 illustrates the E-UTRAN Initial Attach procedure;

FIG. 7 illustrates an Attach procedure in untrusted access;

FIG. 8 illustrates a flow diagram of steps of an embodiment of a method in a user equipment for assigning a cellular network identity;

FIG. 9 illustrates a flow diagram of steps of an embodiment of a method for assisting in attaching a user equipment to a wireless communication

5 network

FIG. 10 illustrates schematically an embodiment of a user equipment;

FIG. 11 illustrates schematically an embodiment of a user equipment;

FIG. 12 illustrates schematically an embodiment of a network node;

FIG. 13 illustrates schematically an embodiment of a network node;

10 FIG. 14 is a schematic block diagram illustrating an embodiment of a user equipment;

FIG. 15 is a schematic block diagram illustrating an embodiment of a user equipment;

15 FIG. 16 is a schematic block diagram illustrating an embodiment of a network node; and

FIG. 17 is a schematic block diagram illustrating an embodiment of a network node.

DETAILED DESCRIPTION

20

Throughout the drawings, the same reference designations are used for similar or corresponding elements.

For a better understanding of the proposed technology, it may be useful to
25 begin with a brief overview of integration of wireless local area networks into mobile core networks of today.

WiFi networks and 3GPP cellular networks are in the present disclosure used as non-limiting exemplifying systems. However, it is emphasized that
30 any type of wireless local area network can be integrated with any type of cellular network according to the same basic principles.

As used herein, the non-limiting terms “mobile station”, “User Equipment” and “wireless device” may refer to a mobile phone, a cellular phone, a

Personal Digital Assistant, PDA, equipped with radio communication capabilities, a smart phone, a laptop or Personal Computer, PC, equipped with an internal or external mobile broadband modem, a tablet PC with radio communication capabilities, a target device, a device to device UE, a
5 machine type UE or UE capable of machine to machine communication, iPad, customer premises equipment, CPE, laptop embedded equipment, LEE, laptop mounted equipment, LME, USB dongle, a portable electronic radio communication device, a sensor device equipped with radio communication capabilities or the like. In particular, the terms “UE” and
10 “STA” and the term “wireless device” should be interpreted as non-limiting terms comprising any type of wireless device communicating with a radio network node in a cellular or mobile communication system or any device equipped with radio circuitry for wireless communication according to any relevant standard for communication within a cellular or mobile
15 communication system.

As used herein, the non-limiting term “network node” may refer to base stations, network control nodes such as network controllers, radio network controllers, base station controllers, and the like. In particular, the term
20 “base station” may encompass different types of radio base stations including standardized base stations such as Node Bs, or evolved Node Bs, eNBs, and also macro/micro/pico radio base stations, home base stations, also known as femto base stations, relay nodes, repeaters, radio access points, base transceiver stations, BTSs, and even radio control nodes
25 controlling one or more Remote Radio Units, RRUs, or the like. The term “network node” may in a similar way also refer to an access point, a Trusted WLAN Access Gateway (TWAG) or an Evolved Packet Data Gateway (ePDG) in a wireless local area network.

30 The UE and network node may also include radio circuitry for communication with one or more other nodes, including transmitting and/or receiving information.

Figure 1A shows the network architecture for E-UTRAN and EPC and how the eNodeB is connected via the S1-interfaces, S1-MME and S1-U to the MME and Serving GW respectively. It also shows how the Wi-Fi access network is connected to the PDN-GW via the S2a interface (that is trusted 5 Wi-Fi access) and to the 3GPP AAA Server via the STa interface.

It should be noted that the configuration of the Wi-Fi network shown in Figure 1 is only an illustrative example and that the Wi-Fi network may be configured or arranged in several other ways and may comprise several 10 further network nodes or entities. For example, the Wi-Fi network may also include a Broadband Network Gateway (BNG). In another example, the Wi-Fi AP may be co-located with a Residential Gateway (RG). In a further example, the Wi-Fi network may also comprise a Trusted WLAN Access Gateway (TWAG). In addition, the interface between the Wi-Fi AC and the PDN GW, 15 i.e. the S2a interface, may also be implemented between the PDN GW and for example either the BNG or the RG.

Untrusted WiFi solution, as illustrated in Fig. 1B, is an overlay solution where IKEv2 and IPsec is used between the UE and EPDG and then the 20 EPDG is connected to AAA (and further on to HSS) for authentication and to PGW via S2b for connectivity. With this solution it is also possible to have automatic authentication using EAP-AKA.

The connection procedure for a STA to a WLAN is depicted in Fig. 2. In this 25 case Radius is used between WiFi network and AAA but according to standard Diameter is used but it is not very common in current products. For the presently presented ideas it is not important if Radius or Diameter is in use.

30 The authentication procedure comprises the following steps:

- 1 The Station (STA) receives a Beacon frame revealing (among other parameters) the security features associated with the Extended Service Set (ESS) the AP belongs to. The format of the beacon frame as

well as all the information elements it carries are described in Chapter 8.3.3.2 of IEEE 802.11;

2 If the STA does not receive a Beacon frame for some reason, it can
generate a Probe Request and send it to the AP. This procedure is
5 called active scanning and by performing it, the STA can receive from
the AP the same information as it would have from a Beacon message.
The Probe Request frame is described in Chapter 8.3.3.9 of IEEE
802.11;

3 The AP answers with Probe Response – IEEE 802.11, Chapter
10 8.3.3.10;

a NOTE: The discovery procedure consists of either step 1 or steps 2
and 3 (i.e., receiving a Beacon frame and exchanging probe messages
are mutually exclusive);

4 The STA sends an Open System Authentication Request as defined in
15 Chapter 11.2.3.2 of IEEE 802.11;

5 The AP responds with an Open System Authentication Response;

6 The STA then sends an Association Request, indicating the security
parameters to be used later;

7 The AP responds with an Association Response

20 a NOTE: The Open System Authentication does not provide any
security. The connection between the STA and the AP is secured at a
later point, by means of Authentication and Key Agreement procedure.
Nevertheless, a possible attack altering the security parameters in the
Open System Authentication message exchange will be detected at the
25 stage of key derivation;

8 At this point the Open System Authentication is completed and the
STA can communicate only with the AP – the rest of the traffic is
blocked by the port-based network control (PBNC) enforcer, as defined
in IEEE 802.1X. Some of the traffic towards external hosts, however,
30 can be forwarded by the AP, as in the case of the communication with
the RADIUS server;

9 This step is the first step of the EAP-SIM authentication RFC 4186.
The AP encapsulates an EAP-Request of Type 18 (SIM) inside an EAP
over LAN (EAPOL) frame, asking the STA to report its identity. In the

- case when the STA is equipped with a SIM, the identity is the International Mobile Subscriber Identity (IMSI), followed by the “@” sign and the home realm. It is also possible for the STA to include an additional “1” in front of the IMSI in order to indicate preference for the exclusive use of EAP-SIM if other EAP methods are available (e.g., EAP-AKAe). This identity can also be a pseudonym/fast re-authentication identity received at an earlier authentication procedure and then it is not possible to extract IMSI from this identity;
- 5 The STA responds with its identity. An example of such is:
10 1234580123000100@wlan.mnc048.mcc264.3gppnetwork.org (and IMSI is in this example 234580123000100 and the preceding “1” indicates the preference to use EAP-SIM);
- 11 The AP extracts the EAP-Response message, encapsulates it in a RADIUS frame and forwards it to the backend AAA server. The
15 handling of EAP frames over RADIUS is described by the Internet Engineering Task Force (IETF) in RFC 3579;
- 12 The AAA server recognizes the EAP method and sends an EAP-Request/SIM/Start, indicating that an EAP-SIM procedure has been initiated for that Supplicant. It also includes the list of supported SIM
20 versions in the message as described in Chapter 10.2 of RFC 4186;
- 13 The AP relays the EAP-Request/SIM/Start message to the STA;
- 14 The STA responds with EAP-Response/SIM/Start message, which carries a random number (NONCE_MT) carried in the AT_NONCE_MT attribute (a randomly selected number), as well as the selected EAP-
25 SIM version (AT_SELECTED_VERSION);
- 15 The AP forwards the EAP-Response/SIM/Start to the AAA server;
- 16 The AAA server obtains the Global System for Mobile communications (GSM) triplet (Random number (RAND), Signal Response (SRES) and Kc) from the Home Location Register/Authentication Centre
30 (HLR/AuC) and derives the keying material as specified in Chapter 7 of RFC 4186. The GSM triplet consists of:
- a RAND – a 128-bit random number, generated by the Authentication Centre (an entity within the GSM core network, used to authenticate subscribers at the point of initial attach) when a subscriber

authentication is requested. Its main use is for the derivation of the Signed Response (SRES) and the Kc;

b SRES – a 32-bit variable, the expected response from the mobile station/STA after it has been challenged with the RAND;

5 c Kc – a 64-bit ciphering key, used to encipher and decipher data transmitted between the STA and the AP;

17 The AAA generates an EAP-Request/SIM/Challenge message, including RAND challenges and message authentication code attribute (AT_MAC). The AT_MAC derivation is based on the RAND and Kc
10 values;

18 The AP forwards the EAP-Request/SIM/Challenge message to the STA;

19 The STA feeds the received RAND into the GSM algorithms running on the SIM and the output is a copy of the AT_MAC and a SRES value.

15 The first thing for the STA to do is to check whether the AT_MAC value received by the AAA (relayed by the AP) and the one generated by the SIM match. If so the STA continues with the authentication, otherwise it responds with an EAP-Response/SIM/Client-Error message. The second thing is to derive a new AT_MAC, based on the generated
20 SRES;

20 The new AT_MAC is sent to the AAA server (via the AP) in an EAP-Response/SIM/Challenge message;

21 The AP forwards the EAP-Response/SIM/Challenge to the AAA server;

22 The AAA server verifies the new AT_MAC value that the STA has just sent. If the verification is successful, it sends an EAP-Success
25 message to the AP. The message also carries keying material – Pairwise Master Key (PMK). The PMK is intended for the AP only and it is not forwarded to the STA (the STA can derive the same key autonomously since it is based on the Kc, which the SIM in the STA
30 can compute based on the RAND);

23 The AP forwards the EAP-Success message to the STA and stores the PMK for the following Four-way handshake;

24 The AP uses the PMK to generate an Authenticator nonce (ANonce);

25 The ANonce value is sent to the STA in an EAPOL-Key message;

- 26 Using the received ANonce (together with the SNonce and the PMK),
the STA constructs the Pairwise Temporal Key (PTK);
- 27 The STA sends an EAPOL-Key message to the AP, including a
Supplicant nonce (SNonce) and a message integrity code (MIC);
- 5 28 The AP uses the ANonce, SNonce and the PMK to construct the PTK.
The AP also uses the MIC in order to verify that the STA has computed
the correct and fresh key. Furthermore, the AP also generates and
installs a Group Temporal Key (GTK, which is used exclusively for the
encryption and decryption of broadcast and multicast traffic;
- 10 29 The AP sends to the STA an encrypted GTK, a sequence number to
use for the next broadcast message and an instruction to install the
PTK (the message is integrity protected by another MIC);
- 30 The STA responds with an acknowledgement message;
- 31 The STA installs both the PTK and the GTK and as of this point uses
15 them to encrypt and decrypt all communication;
- 32 The AP also installs the PTK;
- 33 The 802.1X Controlled Port is now open and the STA can
communicate with other network hosts besides the AP.

20 The current WiFi integration into mobile core is achieved by having separate
authentication for WiFi (via 3GPP-AAA and HSS) and then have the UE
connected via the PGW using either S2a or S2b. The WiFi network is quite
loosely coupled with Mobile Packet Core.

25 It is of interest to use SGSN/MME for combined authentication between
3GPP and WiFi. If the same SGSN/MME that handle authentication for the
UE also for 3GPP is used, see Fig. 3, it is possible for the network to
coordinate between the accesses and make good decisions. This could for
example be that you want the UE to use the access that is “best” based on a
30 number of parameters (e.g., price, user quota, available bandwidth etc.).

If SGSN/MME is used for WiFi authentication, the call-flow will be similar
as in Fig. 2 but with SGSN/MME as AAA and the SGSN/MME can
coordinate the UEs 3GPP access with the UEs WiFi access.

To be able to use the same SGSN/MME for WiFi authentication as that is used for the UE on the 3GPP side, the SGSN/MME have to be identified when UE connects to WiFi. If SGSN/MME is doing the authentication of the 5 UE, it implies that the correct SGSN/MME have to be found already before step 11 in Fig. 2.

In the existing solution in Fig. 2 the IMSI number can be used in step 10 but in that signal it is not always IMSI being sent but it could also be a pseudonym identity. If so, the AAA can request primary identity (i.e., IMSI) 10 but that require extra signalling and it is also a security issue to send IMSI over the air. Also, the IMSI number is only a permanent identity of the UE and can't directly be used to locate the 3GPP node which holds the UE's subscription and MM context. Then there has to be a function (including 15 database) that maps IMSI to 3GPP node.

Embodiments of the proposed technology comprises an assignment of a cellular network identity, e.g. a 3GPP identity, to the UE which can be used, as e.g. EAP-SIM/AKA identity, when connecting to a wireless local area 20 network, e.g. WiFi. The same identity can both be used for trusted (EAP-SIM/AKA inside EAPoL) and untrusted (EAP-AKA in IKEv2) access.

The identity can be assigned to the UE either when it first attaches to the cellular network, e.g. to the 3GPP network, or when it first attaches to the 25 wireless local area network, e.g. WiFi.

The identity will uniquely identify the UE context and in what cellular network node, e.g. 3GPP node, it is attached (SGSN/MME etc.). One particular example could be that the identity is based on the Global Unique 30 Temporary Identifier (GUTI).

By way of example, context information includes information related to a wireless device for establishing and/or maintaining communication in a wireless communication network. A cellular context of the wireless device

includes information for maintaining communication in a cellular radio communication network. A WLAN context of the wireless device includes information for maintaining communication in a WLAN. Context information may for example include state information, security information and/or
5 capability information for a wireless device, and optionally also radio access related information for the wireless device.

In particular, a UE context is a block of information related to UE that includes information useful to maintain communication and/or service in
10 the relevant network, for example UE state information, security information and UE capability information.

The WLAN network node, e.g. the TWAN or ePDG, shall select the authentication node, e.g. the SGSN/MME, based on the cellular network
15 identity, e.g. 3GPP identity, of the UE

The solution can in a data flow sense be divided in two parts; How the UE receives the cellular network identity, e.g. the 3GPP identity and How the UE use the cellular network identity, e.g. the 3GPP identity, so the network can
20 find the correct cellular network node, e.g. 3GPP node. However, the parts are intimately associated to each other into one common concept.

In one embodiment, a method for assigning a cellular network identity, see Fig. 4, starts in step 200. The method comprises identifying, step 206, a
25 user equipment context of a user equipment and in what cellular network node the user equipment is or is going to be attached. The identifying is performed as a response to an attach message from the user equipment in question. The identifying is performed by a network node of a communication network, possibly in cooperation with other network nodes.

30

The network node can in one embodiment be a network node of the cellular network associated with the cellular network identity. The requested information for the identifying process is then available in nodes within the cellular network.

The network node can in another embodiment be a network node of a wireless local area network. The requested information for the identifying process then has to be performed in cooperation with the cellular network.
5 This can be achieved in many different ways and is discussed further below.

In a particular embodiment, the method comprises the further step 202 of determining whether or not the user equipment already has an assigned cellular network identity. As illustrated by 204, if the user equipment does
10 not have the cellular network identity assigned already, step 206 is performed, and consequently the steps following on step 206. Otherwise the process ends.

In the embodiment of Fig. 4, the process continues with step 208, in which
15 a unique representation of the identified user equipment context and the cellular network node is generated. In a step 212, the unique representation is sent to the user equipment.

In a step 210, the unique representation is labelled as a cellular network
20 identity before the step 212 of sending to the user equipment. In this embodiment, the entire cellular network identity, i.e. both the unique representation and the label, is sent to the user equipment.

The process ends in step 219.

25

In a particular embodiment, the wireless local area network is a WiFi network.

In a particular embodiment, the cellular network is a 3GPP cellular network.

30

Fig. 5 illustrates a flow diagram of steps of an embodiment of a method for assigning a cellular network identity. The process starts in step 220. In step 222, a unique representation of a user equipment context of a user equipment and in what cellular network node the user equipment is or is

going to be attached is received in the user equipment in question. The user equipment is capable to attach to a cellular network and to a wireless local area network. This information is received from a network node, e.g. created by the method illustrated in Fig. 4. The network node may be a network node of the cellular network. The network node may also be a network node of the wireless local area network. In step 224, the unique representation is labelled as a cellular network identity. In particular embodiments where the network node provides the labelling, step 224 may be omitted, since the step then becomes redundant. The cellular network identity is in step 226 stored, in this embodiment as a pseudonym or fast re-authentication identity, in a memory in the user equipment. The process ends in step 239.

In an alternative example, step 224 may be omitted. The unique representation may then be stored in a memory without being labelled as a cellular network identity.

In a particular embodiment, the wireless local area network is a WiFi network.

In a particular embodiment, the cellular network is a 3GPP cellular network.

In other words, two alternatives of the UE to receive the cellular network identity, e.g. the 3GPP identity, exist and both can be used at the same time to complement each other.

25

A first solution is that the identity is assigned by a cellular network node, e.g. a 3GPP node, when UE attach to the cellular network, e.g. the 3GPP network. In Fig. 6, the procedure of E-UTRAN initial access is shown and then the MME can assign a temporary UE identity (i.e., GUTI) as for normal attach procedure. The GUTI is typically provided in the Attach Accept step (step 17). UE shall also use the same identity for subsequent non-3GPP access during EAP authentication procedure. This method requires changes in the standard. But such standard changes only changes the UE

behaviour, no standard changes are necessary on network side. However, the network side as such also needs to be changed.

The other method of assigning the 3GPP identity is through the first WiFi authentication procedure. Referring to Fig. 2, the 3GPP identity can be sent as pseudonym or fast re-authentication identity in Radius and EAPOL message (number 17 and 18) containing the EAP-Request/SIM/Challenge. The 3GPP identity can also be sent as pseudonym or fast re-authentication identity in Diameter.

10

RFC4186 specifies:

The server transmits pseudonym usernames and fast re-authentication identities to the peer in cipher, using the AT_ENCR_DATA attribute.

The EAP-Request/SIM/Challenge message MAY include an encrypted pseudonym username and/or an encrypted fast re-authentication identity in the value field of the AT_ENCR_DATA attribute.

For trusted access it is also possible to use EAP-AKA and then the pseudonym and fast re-authentication identity are sent according to RFC4187:

The server transmits pseudonym usernames and fast re-authentication identities to the peer in cipher, using the AT_ENCR_DATA attribute.

The EAP-Request/AKA-Challenge message MAY include an encrypted pseudonym username and/or an encrypted fast re-authentication identity in the value field of the AT_ENCR_DATA attribute. How the network assign 3GPP identity in this solution depend on if the UE is attached to SGSN/MME on 3GPP side or not.

If UE is attached to 3GPP, the network should assign a pseudonym identity and/or fast re-authentication identity that point at the SGSN/MME where the UE context is situated. This could be solved by querying HSS or by broadcasting question to all SGSN/MMEs in the pool. Also other alternatives are possible. However, the exact details of how that is done is

outside the scope for this solution, if they only result in an identification of the SGSN/MME where the UE context is situated.

If UE is not attached to 3GPP, the network should select a SGSN/MME for the UE and provide a 3GPP identity as pseudonym identity that point at the selected SGSN/MME. In one embodiment of this invention the UE can then also use this pseudonym identity as GUTI when attaching to 3GPP and then the attach request will directly be served by the correct SGSN/MME (i.e., where the UE is attached using WiFi).

10

For untrusted access, EAP-AKA is always used and this procedure is depicted in Fig. 7. This procedure is very similar to the trusted access case but IKEv2 is used instead of EAPol. It is the same EAP-AKA protocol inside these “bearer” protocols.

15

Once the user equipment has the cellular network identity stored in a memory, this cellular network identity can be used for attaching to either the cellular network or the wireless local access network.

20 Fig. 8 illustrates a flow diagram of steps of an embodiment of a method for identifying a user equipment upon attaching the user equipment to a wireless communication network. The process starts in step 240. In step 242, a unique representation of a user equipment context of the user equipment and in what cellular network node the user equipment is or is going to be attached is retrieved from a memory in the user equipment.

In particular embodiments, where the unique representation is stored as such, the unique representation is in step 244 labelled as the cellular network identity. The cellular network identity is in this embodiment 30 labelled either a pseudonym identity or a fast re-authentication identity.

In particular embodiments, where the unique representation is stored as a labelled cellular network identity, the step of retrieving 242 comprises retrieving the cellular network identity comprising the unique representation

and a label from the memory in the user equipment. The step 244 may then interpreted as checking that there is a stored label of either a pseudonym identity or a fast re-authentication identity.

5 In step 246, the cellular network identity comprising the unique representation is sent as a user identity, in the form of a pseudonym identity or a fast re-authentication identity, in an attach procedure to the wireless communication network. The process ends in step 259.

10 The wireless communication network is in one embodiment the cellular network associated with the cellular network identity.

The wireless communication network is in another embodiment a wireless local area network.

15

In a particular embodiment, the step of sending 246 comprises sending the cellular network identity as a pseudonym identity or a fast re-authentication identity in an Extensible Authentication Protocol.

20 In a particular embodiment, the wireless local area network is a WiFi network.

In a particular embodiment, the cellular network is a 3GPP cellular network.

25 At the network side, a receiving process is provided.

Fig. 9 illustrates a flow diagram of steps of an embodiment of a method for assisting in attaching a user equipment to a wireless communication network. The process starts in step 260. In step 262, a user identity is
30 received in a network node from a user equipment. In particular embodiments, this receiving is a part of an attach procedure. The step of receiving comprises receiving of the cellular network identity as a username which is equal to a pseudonym identity or a fast re-authentication identity, e.g. in an Extensible Authentication Protocol. In step 264, it is determined

whether or not the received user identity is a cellular network identity comprising a unique representation of a user equipment context of the user equipment and in what cellular network node the user equipment is or is going to be attached. In a particular embodiment, the step of determining
5 comprises identification of a labelling of the cellular network identity. If it is determined that the received user identity is a cellular network identity, as illustrated by step 266, step 268 is performed, in which an authentication procedure is directed towards an authentication node defined by the cellular network identity. The process ends in step 279.

10

In a particular embodiment, the network node is a network node of the cellular network associated with the cellular network identity.

In another particular embodiment, the network node is a network node of a
15 wireless local area network.

In a particular embodiment, the wireless local area network is a WiFi network.

20 In a particular embodiment, the cellular network is a 3GPP cellular network.

In one embodiment, the UE use of the cellular network identity, e.g. the 3GPP identity, is performed compatible with 802.11 standards. However, when the UE receives the pseudonym or fast re-authentication identity it
25 should use these as identity at the next authentication procedure or fast re-authentication procedure. At that time the access network (e.g., TWAG in the case of trusted access or ePDG in the case of untrusted access) can directly use the 3GPP identity to find the 3GPP node (e.g., SGSN/MME).

30 The particular format of the cellular network identity, e.g. the 3GPP identity, is not very crucial for the here presented technology to operate, as such, however, it is an advantage if already existing parameters may be used. The cellular network identity may for instance be formed similar to a pseudonym identity. The pseudonym identity is a string that can be formatted in any

way. One way to format the cellular network identity is to just use the GUTI value of the UE or any representation thereof.

The format can as mentioned above also comprise a labelling. In one embodiment, this label may be a prefix that indicate to TWAG/ePDG if pseudonym identity contain a cellular network identity, e.g. a 3GPP identity, and TWAG/ePDG shall therefore select SGSN/MME based on 3GPP identity. If the prefix is not present, TWAG/ePDG shall choose AAA as in the legacy solution.

10

It will be appreciated that the methods and devices described herein can be combined and re-arranged in a variety of ways.

For example, embodiments may be implemented in hardware, or in software for execution by suitable processing circuitry, or a combination thereof.

The steps, functions, procedures, modules and/or blocks described herein may be implemented in hardware using any conventional technology, such as discrete circuit or integrated circuit technology, including both general-purpose electronic circuitry and application-specific circuitry.

Particular examples include one or more suitably configured digital signal processors and other known electronic circuits, e.g. discrete logic gates interconnected to perform a specialized function, or Application Specific Integrated Circuits (ASICs).

Alternatively, at least some of the steps, functions, procedures, modules and/or blocks described herein may be implemented in software such as a computer program for execution by suitable processing circuitry such as one or more processors or processing units.

The flow diagram or diagrams presented herein may therefore be regarded as a computer flow diagram or diagrams, when performed by one or more processors. A corresponding apparatus may be defined as a group of

function modules, where each step performed by the processor corresponds to a function module. In this case, the function modules are implemented as a computer program running on the processor.

5 Examples of processing circuitry includes, but is not limited to, one or more microprocessors, one or more Digital Signal Processors, DSPs, one or more Central Processing Units, CPUs, video acceleration hardware, and/or any suitable programmable logic circuitry such as one or more Field Programmable Gate Arrays, FPGAs, or one or more Programmable Logic
10 Controllers, PLCs.

It should also be understood that it may be possible to re-use the general processing capabilities of any conventional device or unit in which the proposed technology is implemented. It may also be possible to re-use
15 existing software, e.g. by reprogramming of the existing software or by adding new software components.

Fig. 10 illustrates schematically an embodiment of a user equipment 20. The user equipment 20 is capable to attach to a cellular network and to a
20 wireless local area network. The user equipment 20 comprises an input, illustrated as an I/O bus 304 and an I/O controller 303. The user equipment 20 further comprises a processor 301, a memory 302 and a system bus 300 for communication between the different parts. The memory 302 comprises instructions, illustrated as software entities 311-313;
25 software for receiving a unique representation from a network node, software for labelling the unique representation as a cellular network identity and software for storing the cellular network identity in the memory 302. The instructions are executable by the processor 301 whereby the user equipment 20 is operative to receive a unique representation of a user
30 equipment context of the user equipment and in what cellular network node the user equipment is or is going to be attached. This unique representation is received from a network node via the input, in this embodiment the I/O bus 304 and the I/O controller 303. The user equipment 20 is by the instructions further operative to label the unique representation as a

cellular network identity and to store the cellular network identity in the memory.

In a particular example, where the network node provides the unique
5 representation already labeled as a cellular network identity, the software
for labelling the unique representation as a cellular network identity is
omitted.

In a particular embodiment, the network node is a network node of the
10 cellular network.

In a particular embodiment, the network node is a network node of the
wireless local area network.

15 In a particular embodiment, the wireless local area network is WiFi network.

In a particular embodiment, the cellular network is a 3GPP cellular network.

Fig. 11 illustrates schematically an embodiment of a user equipment 20.
20 The user equipment 20 is capable to attach to a cellular network and to a
wireless local area network. The user equipment 20 comprises an output,
illustrated as an I/O bus 304 and an I/O controller 303. The user
equipment 20 further comprises a processor 301, a memory 302 and a
system bus 300 for communication between the different parts. The memory
25 302 comprises instructions, illustrated as software entities 321-323;
software for retrieving a unique representation from the memory 302,
software for labelling the unique representation as a cellular network
identity and software for sending the cellular network identity to the
wireless communication network. The instructions are executable by the
30 processor 301 whereby the user equipment 20 is operative to retrieve, from
the memory 302, a unique representation of a user equipment context of the
user equipment and in what cellular network node the user equipment is or
is going to be attached. The user equipment 20 is by the instructions further
operative to label the unique representation as the cellular network identity.

The user equipment 20 is by the instructions further operative to send, via the output, in this particular embodiment the I/O bus 304 and the I/O controller 303, a cellular network identity comprising the unique representation as a user identity in an attach procedure to the wireless
5 communication network.

In a particular embodiment, where the cellular network identity is stored in the memory 302, the instructions causes the user equipment to be further operative to retrieve the cellular network identity comprising the unique
10 representation and a label thereof from the memory 302 in the user equipment 20. The software 322 for labelling the unique representation as a cellular network identity may then be omitted.

In a particular embodiment, the wireless communication network is the
15 cellular network associated with the cellular network identity.

In a particular embodiment, the wireless communication network is a wireless local area network.

20 In a particular embodiment, the user equipment is further operative by the software 323 software for sending the cellular network identity to the wireless communication network to send the cellular network identity as a pseudonym identity or a fast re-authentication identity in an Extensible Authentication Protocol.

25

In a particular embodiment, the wireless local area network is WiFi network.

In a particular embodiment, the cellular network is a 3GPP cellular network.

30 Fig. 12 illustrates schematically an embodiment of a network node 30 of a communication network. The network node 30 comprises an input, and an output, illustrated in common as an I/O bus 354 and an I/O controller 353. The network node 30 further comprises a processor 351, a memory 352 and a system bus 350 for communication between the different parts. The

memory 352 comprises instructions, illustrated as software entities 361-365; software for determining whether or not the user equipment already has an assigned cellular network identity, software for identifying a user equipment context of the user equipment and in what cellular network node 5 the user equipment is or is going to be attached, software for generating a unique representation of the identified user equipment context and the cellular network node, software for labelling the unique representation as a cellular network identity and software for sending the unique representation to the user equipment. The instructions are executable by the processor 351 10 whereby the network node 30 is operative to identify, as a response to an attach message from a user equipment, a user equipment context of the user equipment and in what cellular network node the user equipment is or is going to be attached. The network node 30 is further operative to generate a unique representation of the identified user equipment context and the 15 cellular network node. The network node 30 is further operative to send the unique representation via the output to the user equipment.

In particular embodiments, the software for determining whether or not the user equipment already has an assigned cellular network identity may be 20 omitted.

In particular embodiments having the software for determining whether or not the user equipment already has an assigned cellular network identity, the network node 30 is operative to determine whether or not the user 25 equipment already has an assigned cellular network identity, whereby the identifying, generating and sending are performed if the user equipment already does not have the cellular network identity assigned.

In particular embodiments, the software for labelling the unique 30 representation as a cellular network identity may be omitted.

In particular embodiments having the software for labelling the unique representation as a cellular network identity, the network node 30 is operative to label the unique representation as a cellular network identity.

In a particular embodiment, the network node 30 is a network node of the cellular network associated with the cellular network identity.

5 In another particular embodiment, the network node 30 is a network node of a wireless local area network.

In a particular embodiment, the wireless local area network is WiFi network.

10 In a particular embodiment, the cellular network is a 3GPP cellular network.

Fig. 13 illustrates schematically an embodiment of a network node 30 of a communication network. The network node 30 comprises an input, and an output, illustrated in common as an I/O bus 354 and an I/O controller 353.

15 The network node 30 further comprises a processor 351, a memory 352 and a system bus 350 for communication between the different parts. The memory 352 comprises instructions, illustrated as software entities 371-373; software for receiving a user identity from a user equipment, software for determining whether or not the received user identity is a cellular

20 network identity and software for directing, if determined that the received user identity is a cellular network identity, an authentication procedure towards an authentication node defined by the cellular network identity. The instructions are executable by the processor 351 whereby the network node 30 is operative to receive a user identity from a user equipment via the

25 input. The network node 30 is further operative to determine whether or not the received user identity is a cellular network identity comprising a unique representation of a user equipment context of the user equipment and in what cellular network node the user equipment is or is going to be attached. The network node 30 is further operative to direct, if determined that the

30 received user identity is a cellular network identity, an authentication procedure towards an authentication node defined by the cellular network identity.

In a particular embodiment, the software 372 for determining whether or not the received user identity is a cellular network identity causes the network node 30 to be further operative to identify a labelling of the cellular network identity.

5

In a particular embodiment, the network node 30 is a network node of the cellular network associated with the cellular network identity.

In a particular embodiment, the network node is a network node of a
10 wireless local area network.

In a particular embodiment, the software 371 for receiving a user identity from a user equipment causes the network node to be further operative to receive the cellular network identity as a pseudonym identity or a fast re-
15 authentication identity in an Extensible Authentication Protocol.

In a particular embodiment, the wireless local area network is WiFi network.

In a particular embodiment, the cellular network is a 3GPP cellular network.
20

Above, examples of computer implementations were described. The network node and user equipment, respectively, comprises processing circuitry such as one or more processors and a memory. In these particular examples, at least some of the steps, functions, procedures, modules and/or blocks
25 described herein are implemented in a computer program, which is loaded into the memory for execution by the processing circuitry. The processing circuitry and memory are interconnected to each other to enable normal software execution. An optional input/output device may also be interconnected to the processing circuitry and/or the memory to enable
30 input and/or output of relevant data such as input parameter(s) and/or resulting output parameter(s).

The term 'computer' should be interpreted in a general sense as any system or device capable of executing program code or computer program

instructions to perform a particular processing, determining or computing task.

In a particular embodiment, the computer program comprises instructions, 5 which when executed by at least one processor, cause the processor(s) to perform different operations. The computer program resides in a memory.

In one embodiment, the computer program comprising program code, which when executed by a processing circuitry causes the processing circuitry to 10 receive, from a network node via an input, a unique representation of a user equipment context of the user equipment and in what cellular network node the user equipment is or is going to be attached, to label the unique representation as a cellular network identity, and to store the cellular network identity in the memory.

15

In one embodiment, the computer program comprising program code, which when executed by a processing circuitry causes the processing circuitry to retrieve, from a memory, a unique representation of a user equipment context of the user equipment and in what cellular network node the user 20 equipment is or is going to be attached, and to send, via an output, a cellular network identity comprising the unique representation as a user identity in an attach procedure to the wireless communication network.

In one embodiment, the computer program comprising program code, which 25 when executed by a processing circuitry causes the processing circuitry to identify, as a response to an attach message from a user equipment, a user equipment context of the user equipment and in what cellular network node the user equipment is or is going to be attached, to generate a unique representation of the identified user equipment context and the cellular 30 network node, and to send the unique representation via the output to the user equipment.

In one embodiment, the computer program comprising program code, which when executed by a processing circuitry causes the processing circuitry to

receive a user identity from a user equipment via an input, to determine whether or not the received user identity is a cellular network identity comprising a unique representation of a user equipment context of the user equipment and in what cellular network node the user equipment is or is
5 going to be attached, and to direct, if determined that the received user identity is a cellular network identity, an authentication procedure towards an authentication node defined by the cellular network identity.

The proposed technology also provides a carrier comprising the computer
10 program, wherein the carrier is one of an electronic signal, an optical signal, an electromagnetic signal, a magnetic signal, an electric signal, a radio signal, a microwave signal, or a computer-readable storage medium.

The software or computer program may thus be realized as a computer
15 program product, which is normally carried or stored on a computer-readable medium. The computer-readable medium may include one or more removable or non-removable memory devices including, but not limited to a Read-Only Memory, ROM, a Random Access Memory, RAM, a Compact Disc, CD, a Digital Versatile Disc, DVD, a Blu-ray disc, a Universal Serial Bus, USB,
20 memory, a Hard Disk Drive, HDD storage device, a flash memory, a magnetic tape, or any other conventional memory device. The computer program may thus be loaded into the operating memory of a computer or equivalent processing device for execution by the processing circuitry thereof.

25 In one embodiment, a computer program product comprises a computer-readable medium on which a computer program is stored. The computer program comprises program code, which when executed by a processing circuitry causes the processing circuitry to receive, from a network node via the input, a unique representation of a user equipment context of the user
30 equipment and in what cellular network node the user equipment is or is going to be attached, to label the unique representation as a cellular network identity and to store the cellular network identity in the memory.

In one embodiment, a computer program product comprising a computer-readable medium on which a computer program is stored. The computer program comprises program code, which when executed by a processing circuitry causes the processing circuitry to retrieve, from a memory, a
5 unique representation of a user equipment context of the user equipment and in what cellular network node the user equipment is or is going to be attached, and to send, via an output, a cellular network identity comprising the unique representation as a user identity in an attach procedure to the wireless communication network.

10

In one embodiment, a computer program product comprises a computer-readable medium on which a computer program is stored, which computer program comprises program code, which when executed by a processing circuitry causes the processing circuitry to identify, as a response to an
15 attach message from a user equipment, a user equipment context of the user equipment and in what cellular network node the user equipment is or is going to be attached, to generate a unique representation of the identified user equipment context and the cellular network node, and to send the unique representation via the output to the user equipment.

20

In one embodiment, a computer program product comprises a computer-readable medium on which a computer program is stored. The computer program comprises program code, which when executed by a processing circuitry causes the processing circuitry to receive a user identity from a
25 user equipment via the input, to determine whether or not the received user identity is a cellular network identity comprising a unique representation of a user equipment context of the user equipment and in what cellular network node the user equipment is or is going to be attached, and to direct, if determined that the received user identity is a cellular network identity,
30 an authentication procedure towards an authentication node defined by the cellular network identity.

The network node and user equipment, respectively, is thus configured to perform, when executing the computer program, well-defined processing tasks such as those described herein.

5 The computer or processing circuitry does not have to be dedicated to only execute the above-described steps, functions, procedure and/or blocks, but may also execute other tasks.

As indicated herein, the user equipment and/or network node may
10 alternatively be defined as a group of function modules, where the function modules are implemented as a computer program running on at least one processor.

The computer program residing in memory may thus be organized as
15 appropriate function modules configured to perform, when executed by the processor, at least part of the steps and/or tasks described herein. Examples of such function modules are illustrated in Figures 14-17.

Figure 14 is a schematic block diagram illustrating an example of a user
20 equipment 20 comprising a group of function modules. The user equipment 20 is capable to attach to a cellular network and a wireless local area network. The user equipment comprises a receiving module 401 for receiving a unique representation of a user equipment context of the user equipment and in what cellular network node the user equipment is or is
25 going to be attached, from a network node. The user equipment may further comprises a labelling module 402 for labelling the unique representation as a cellular network identity. The user equipment further comprises a memory 302. The user equipment further comprises a storing module 403 for storing the cellular network identity in the memory 302.

30

Figure 15 is a schematic block diagram illustrating an example of a user equipment 20 comprising a group of function modules. The user equipment 20 is capable to attach to a cellular network and a wireless local area network. The user equipment comprises a memory 302. The user equipment

further comprises a retrieving module 411 for retrieving, from the memory 302, a unique representation of a user equipment context of the user equipment and in what cellular network node the user equipment is or is going to be attached. The user equipment comprises a labelling module 412
5 for labelling the unique representation as a cellular network identity. The user equipment further comprises a sending module 413 for sending a cellular network identity comprising the unique representation as a user identity in an attach procedure to the wireless communication network.

10 Figure 16 is a schematic block diagram illustrating an example of a network node 30 in a wireless communication network comprising a group of function modules. The network node 30 comprises an identifying module 422 for identifying, as a response to an attach message from a user equipment, a user equipment context of the user equipment and in what
15 cellular network node the user equipment is or is going to be attached. The network node 30 further comprises a generating module 423 for generating a unique representation of the identified user equipment context and the cellular network node. The network node 30 further comprises a sending module 425 for sending the unique representation to the user equipment.
20 The network node 30 may optionally comprise a determining module 421 for determining whether or not the user equipment already has an assigned cellular network identity. Network node 30 comprises a labelling module 424 for labelling the unique representation as a cellular network identity.

25 Figure 17 is a schematic block diagram illustrating an example of a network node 30 in a wireless communication network comprising a group of function modules. The network node 30 comprises a receiving module 431 for receiving a user identity from a user equipment. The network node 30 further comprises a determining module 432 for determining whether or not
30 the received user identity is a cellular network identity comprising a unique representation of a user equipment context of the user equipment and in what cellular network node the user equipment is or is going to be attached. The network node 30 further comprises a directing module 433 for directing, if determined that the received user identity is a cellular network identity,

an authentication procedure towards an authentication node defined by the cellular network identity.

The present presentation propose that the network should provide a 3GPP
5 identity as pseudonym or fast re-authentication ID to the UE so that the network can easily find the 3GPP node and context when UE do attach procedure (trusted or untrusted) on WLAN. By using this solution it is possible for the network to locate the UE context early in the attach procedure and coordinate between 3GPP and WiFi access.

10

The embodiments described above are merely given as examples, and it should be understood that the proposed technology is not limited thereto. It will be understood by those skilled in the art that various modifications, combinations and changes may be made to the embodiments without
15 departing from the present scope as defined by the appended claims. In particular, different part solutions in the different embodiments can be combined in other configurations, where technically possible.

<u>Abbreviation</u>	<u>Explanation</u>
20 3GPP	3 rd Generation Partnership Project
AAA	Authentication Authorization Accounting
AKA	Authentication and Key Agreement
AP	Access Point
APN	Access Point Name
25 ASIC	Application Specific Integrated Circuit
BNG	Broadband Network Gateway
BTS	Base Transceiver Station
CD	Compact Disc
CPE	Customer Premises Equipment
30 CPU	Central Processing Unit
DSP	Digital Signal Processor
DVD	Digital Versatile Disc
EAP	Extensible Authentication Protocol
EAPOL	EAP over LAN

EPC	Evolved Packet Core
ePDG	Evolved Packet Data Gateway
ESS	Extended Service Set
E-UTRAN	Evolved Universal Terrestrial Radio Access Network
5 FPGA	Field Programmable Gate Array
GSM	Global System for Mobile communications
GTK	Group Temporal Key
GUTI	Global Unique Temporary Identifier
GW	Gateway
10 HDD	Hard Disk Drive
HLR/AuC	Home Location Register/Authentication Centre
HSS	Home Subscriber Server
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
15 IMSI	International Mobile Subscriber Identity
IPsec	IP security
LEE	Laptop Embedded Equipment
LME	Laptop Mounted Equipment
MIC	Message Integrity Code
20 MME	Mobility Management Entity
NAT	Network Address Translator
PBNC	Port-Based Network Control
PC	Personal Computer
PDA	Personal Digital Assistant
25 PDN	Packet Data Network
PGW, PDN-GW	PDN Gateway
PLC	Programmable Logic Controller
PLMN	Public Land Mobile Network
PMK	Pairwise Master Key
30 PTK	Pairwise Temporal Key
RAM	Random Access Memory
RAND	Random number
RG	Residential Gateway
RNC	Radio Network Controller

ROM	Read-Only Memory
RRU	Remote Radio Unit
RSN	Retransmission Sequence Number
SA	Security Association
5 SGSN	Serving General packet radio services Support Node
SNounce	Supplicant Nounce
SIM	Subscriber Identity Module
SRES	Signal RESponse
SSID	Service Set Identifier
10 STA	Station
TWAG	Trusted WLAN Access Gateway
UE	User Equipment
USB	Universal Serial Bus
VPLMN	Visited PLMN
15 WLAN	Wireless Local Area Network

CLAIMS

1. A method for assigning a cellular network identity, comprising the steps of:
 - 5 - identifying (206), by a network node of a communication network as a response to an attach message from a user equipment, a user equipment context of said user equipment and in what cellular network node said user equipment is or is going to be attached;
 - generating (208) a unique representation of said identified user
10 equipment context and said cellular network node;
 - labelling (210) said unique representation as a cellular network identity, said cellular network identity being one of a pseudonym identity and a fast re-authentication identity; and
 - sending (212) said unique representation to said user equipment as
15 said one of a pseudonym identity and a fast re-authentication identity.
2. The method according to claim 21, **characterized by** the further step of:
 - determining whether or not said user equipment already has an
20 assigned cellular network identity;whereby said steps of identifying (206), generating (208), labelling (210) and sending (212) are performed if said user equipment already does not have said cellular network identity assigned.
- 25 3. The method according to claim 1 or 2, **characterized in that** said network node is a network node of the cellular network associated with said cellular network identity.
4. The method according to claim 1 or 2, **characterized in that** said
30 network node is a network node of a wireless local area network.
5. The method according to any of the claims 1 to 4, **characterized in that** said step of sending is performed using at least one protocol of:
Radius;

Diameter;
EAPOL;
IKEv2;
EAP-SIM; and
5 EAP-AKA.

6. A method for assigning a cellular network identity, comprising the steps of:

- receiving (222), in a user equipment capable to attach to a cellular
10 network and a wireless local area network, a unique representation of a user equipment context of said user equipment and in what cellular network node said user equipment is or is going to be attached, from a network node;
- labelling (224) said unique representation as a cellular network
15 identity; and
- storing (226) said cellular network identity as at least one of a pseudonym identity and a fast re-authentication identity in a memory in said user equipment.

20 7. A method for identifying a user equipment upon attaching said user equipment to a wireless communication network, comprising the steps of:

- retrieving (242), from a memory in said user equipment, a unique representation of a user equipment context of said user equipment and in what cellular network node said user equipment is or is going to be
25 attached;
- labelling (244) said unique representation as a cellular network identity, said cellular network identity being one of a pseudonym identity and a fast re-authentication identity;
- sending (246) a cellular network identity comprising said unique
30 representation as a user identity in an attach procedure to said wireless communication network.

8. A method for assisting in attaching a user equipment to a wireless communication network, comprising the steps of:

- receiving (266), in a network node, a user identity from a user equipment;
- determining (264) whether or not said received user identity is a cellular network identity, being one of a pseudonym identity and a fast re-authentication identity comprising a unique representation of a user equipment context of said user equipment and in what cellular network node said user equipment is or is going to be attached; and
- directing (268), if determined that said received user identity is a cellular network identity, an authentication procedure towards an authentication node defined by said cellular network identity.

9. The method according to any of the claims 1 to 8, **characterized in that** said wireless local area network is WiFi network.

10. The method according to any of the claims 1 to 8, **characterized in that** said cellular network is a 3GPP cellular network.

11. A network node (30) of a communication network, said network node (30) comprising an input (354), a processor (351), a memory (352) and an output (354), said memory (352) comprising instructions (361-365) executable by said processor (351) whereby said network node (30) is operative to:

- identify, as a response to an attach message from a user equipment (20), a user equipment context of said user equipment (20) and in what cellular network node said user equipment is or is going to be attached;
- generate a unique representation of said identified user equipment context and said cellular network node;
- label said unique representation as a cellular network identity, said cellular network identity being one of a pseudonym identity and a fast re-authentication identity; and to
- send said unique representation via said output (354) to said user equipment (20) as said one of a pseudonym identity and a fast re-authentication identity.

12. The network node according to claim 11, **characterized in that** said instructions (361-365) causes the network node (30) to be further operative to:

5 - determine whether or not said user equipment (20) already has an assigned cellular network identity;

whereby said identifying, generating and sending are performed if said user equipment (20) already does not have said cellular network identity assigned.

10

13. The network node according to claim 11 or 12, **characterized in that** said network node (30) is a network node of the cellular network associated with said cellular network identity.

15 14. The network node according to claim 11 or 12, **characterized in that** said network node (30) is a network node of a wireless local area network.

15. The network node according to any of the claims 11 to 14,
20 **characterized in that** said memory (352) comprising further instructions (361-365) executable by said processor (351) whereby said network node (30) is operative to send said unique representation using at least one protocol of:

Radius;

25 Diameter;

EAPOL;

IKEv2;

EAP-SIM; and

EAP-AKA.

30

16. A network node (30) of a communication network, said network node (30) comprising an input (354), a processor (351), a memory (352) and an output (354), said memory (352) comprising instructions (371-373)

executable by said processor (351) whereby said network node (30) is operative to:

- receive a user identity from a user equipment (20) via said input (354);
- 5 - determine whether or not said received user identity is a cellular network identity, being one of a pseudonym identity and a fast re-authentication identity comprising a unique representation of a user equipment context of said user equipment and in what cellular network node said user equipment is or is going to be attached; and
- 10 - direct, if determined that said received user identity is a cellular network identity, an authentication procedure towards an authentication node defined by said cellular network identity.

17. The network node according to any of the claims 11 to 16,
15 **characterized in that** said wireless local area network is WiFi network.

18. The network node according to any of the claims 11 to 16,
characterized in that said cellular network is a 3GPP cellular network.

20 19. A user equipment (20) capable to attach to a cellular network and a wireless local area network, said user equipment comprising an input (304), a processor (301) and a memory (302), said memory (303) comprising instructions (311-313) executable by said processor (301) whereby said user equipment (20) is operative to:

- 25 - receive, from a network node via said input, a unique representation of a user equipment context of said user equipment and in what cellular network node said user equipment is or is going to be attached;
- label said unique representation as a cellular network identity; and
- store said cellular network identity as at least one of a pseudonym
30 identity and a fast re-authentication identity in said memory (302).

20. A user equipment (20) capable to attach to a cellular network and a wireless local area network, said user equipment (20) comprising a processor (301), a memory (302) and an output (304), said memory (302)

comprising instructions (321-323) executable by said processor (301) whereby said user equipment (20) is operative to:

- retrieve, from said memory (302), a unique representation of a user equipment context of said user equipment (20) and in what cellular network node said user equipment is or is going to be attached;
- label said unique representation as a cellular network identity, said cellular network identity being one of a pseudonym identity and a fast re-authentication identity; and to
- send, via said output (304), a cellular network identity comprising said unique representation as a user identity in an attach procedure to said wireless communication network.

21. The user equipment according to claim 19 or 20, **characterized in that** said wireless local area network is WiFi network.

15

22. The user equipment according to claim 19 or 20, **characterized in that** said cellular network is a 3GPP cellular network.

23. A network node (30) in a wireless communication network, comprising:

- an identifying module (422) for identifying, as a response to an attach message from a user equipment (20), a user equipment context of said user equipment (20) and in what cellular network node said user equipment (20) is or is going to be attached;
- 25 - a generating module (423) for generating a unique representation of said identified user equipment context and said cellular network node;
- a labelling module (424) for labelling said unique representation as a cellular network identity, said cellular network identity being one of a pseudonym identity and a fast re-authentication identity; and
- 30 - a sending module (425) for sending said unique representation to said user equipment (20) as said one of a pseudonym identity and a fast re-authentication identity.

24. A user equipment (20) capable to attach to a cellular network and a wireless local area network, said user equipment (20) comprising:

- a receiving module (401) for receiving a unique representation of a user equipment context of said user equipment and in what cellular network node said user equipment is or is going to be attached, from a network node;
- a labelling module (402) for labelling said unique representation as a cellular network identity;
- a memory (302); and
- 10 - a storing module (403) for storing said cellular network identity as at least one of a pseudonym identity and a fast re-authentication identity in said memory (302).

25. A user equipment (20) capable to attach to a cellular network and a wireless local area network, said user equipment (20) comprising:

- a memory (302);
- a retrieving module (411) for retrieving, from said memory (302), a unique representation of a user equipment context of said user equipment (20) and in what cellular network node said user equipment is or is going to be attached;
- a labelling module (412) for labelling said unique representation as a cellular network identity, said cellular network identity being one of a pseudonym identity and a fast re-authentication identity; and
- a sending module (413) for sending a cellular network identity comprising said unique representation as a user identity in an attach procedure to said wireless communication network.

26. A network node (30) in a wireless communication network, comprising:

- 30 - a receiving module (431) for receiving a user identity from a user equipment (20);
- a determining module (432) for determining whether or not said received user identity is a cellular network identity, being one of a pseudonym identity and a fast re-authentication identity comprising a

unique representation of a user equipment context of said user equipment and in what cellular network node said user equipment is or is going to be attached; and

- a directing module (433) for directing, if determined that said 5 received user identity is a cellular network identity, an authentication procedure towards an authentication node defined by said cellular network identity.

27. A computer program, residing in a memory (352), said computer 10 program comprising program code, which when executed by a processing circuitry causes the processing circuitry to:

- identify, a as a response to an attach message from a user equipment (20), a user equipment context of said user equipment (20) and in what cellular network node said user equipment (20) is or is going to be 15 attached;
- generate a unique representation of said identified user equipment context and said cellular network node;
- label said unique representation as a cellular network identity, said cellular network identity being one of a pseudonym identity and a fast re- 20 authentication identity; and to
- send said unique representation via an output to said user equipment (20) as said one of a pseudonym identity and a fast re-authentication identity.

25 28. A computer program, residing in a memory (302), said computer program comprising program code, which when executed by a processing circuitry causes the processing circuitry to:

- receive, from a network node (30) via an input, a unique representation of a user equipment context of a user equipment (20) and in 30 what cellular network node said user equipment (20) is or is going to be attached;
- label said unique representation as a cellular network identity; and
- store said cellular network identity as at least one of a pseudonym identity and a fast re-authentication identity in said memory.

29. A computer program, residing in a memory (302), said computer program comprising program code, which when executed by a processing circuitry causes the processing circuitry to:

- 5 - retrieve, from said memory, a unique representation of a user equipment context of a user equipment (20) and in what cellular network node said user equipment (20) is or is going to be attached;
- label said unique representation as a cellular network identity, said cellular network identity being one of a pseudonym identity and a fast re-
10 authentication identity; and to
- send, via an output, a cellular network identity comprising said unique representation as a user identity in an attach procedure to said wireless communication network.

15 30. A computer program, residing in a memory (352), said computer program comprising program code, which when executed by a processing circuitry causes the processing circuitry to:

- receive a user identity from a user equipment (20) via an input;
- determine whether or not said received user identity is a cellular
20 network identity, being one of a pseudonym identity and a fast re-authentication identity comprising a unique representation of a user equipment context of said user equipment and in what cellular network node said user equipment is or is going to be attached; and
- direct, if determined that said received user identity is a cellular
25 network identity, an authentication procedure towards an authentication node defined by said cellular network identity.

31. A computer program product, comprising a computer-readable medium on which a computer program is stored, which computer program
30 comprises program code, which when executed by a processing circuitry causes the processing circuitry to:

- identify, as a response to an attach message from a user equipment (20), a user equipment context of said user equipment (20) and

in what cellular network node said user equipment (20) is or is going to be attached;

- generate a unique representation of said identified user equipment context and said cellular network node;
- 5 - label said unique representation as a cellular network identity, said cellular network identity being one of a pseudonym identity and a fast re-authentication identity; and to
- send said unique representation via an output to said user equipment (20) as said one of a pseudonym identity and a fast re-
- 10 authentication identity.

32. A computer program product, comprising a computer-readable medium on which a computer program is stored, which computer program comprises program code, which when executed by a processing circuitry

15 causes the processing circuitry to:

- receive, from a network node (30) via an input, a unique representation of a user equipment context of a user equipment (20) and in what cellular network node said user equipment (20) is or is going to be attached;
- 20 - label said unique representation as a cellular network identity; and
- store said cellular network identity as at least one of a pseudonym identity and a fast re-authentication identity in a memory.

33. A computer program product, comprising a computer-readable

25 medium on which a computer program is stored, which computer program comprises program code, which when executed by a processing circuitry causes the processing circuitry to:

- retrieve, from a memory, a unique representation of a user equipment context of a user equipment (20) and in what cellular network
- 30 node said user equipment (20) is or is going to be attached;
- label said unique representation as a cellular network identity, said cellular network identity being one of a pseudonym identity and a fast re-authentication identity; and to

- send, via an output, a cellular network identity comprising said unique representation as a user identity in an attach procedure to said wireless communication network.

5 34. A computer program product, comprising a computer-readable medium on which a computer program is stored, which computer program comprises program code, which when executed by a processing circuitry causes the processing circuitry to:

- receive a user identity from a user equipment (20) via an input;
- 10 - determine whether or not said received user identity is a cellular network identity, being one of a pseudonym identity and a fast re-authentication identity comprising a unique representation of a user equipment context of said user equipment and in what cellular network node said user equipment is or is going to be attached; and
- 15 - direct, if determined that said received user identity is a cellular network identity, an authentication procedure towards an authentication node defined by said cellular network identity.

1/21

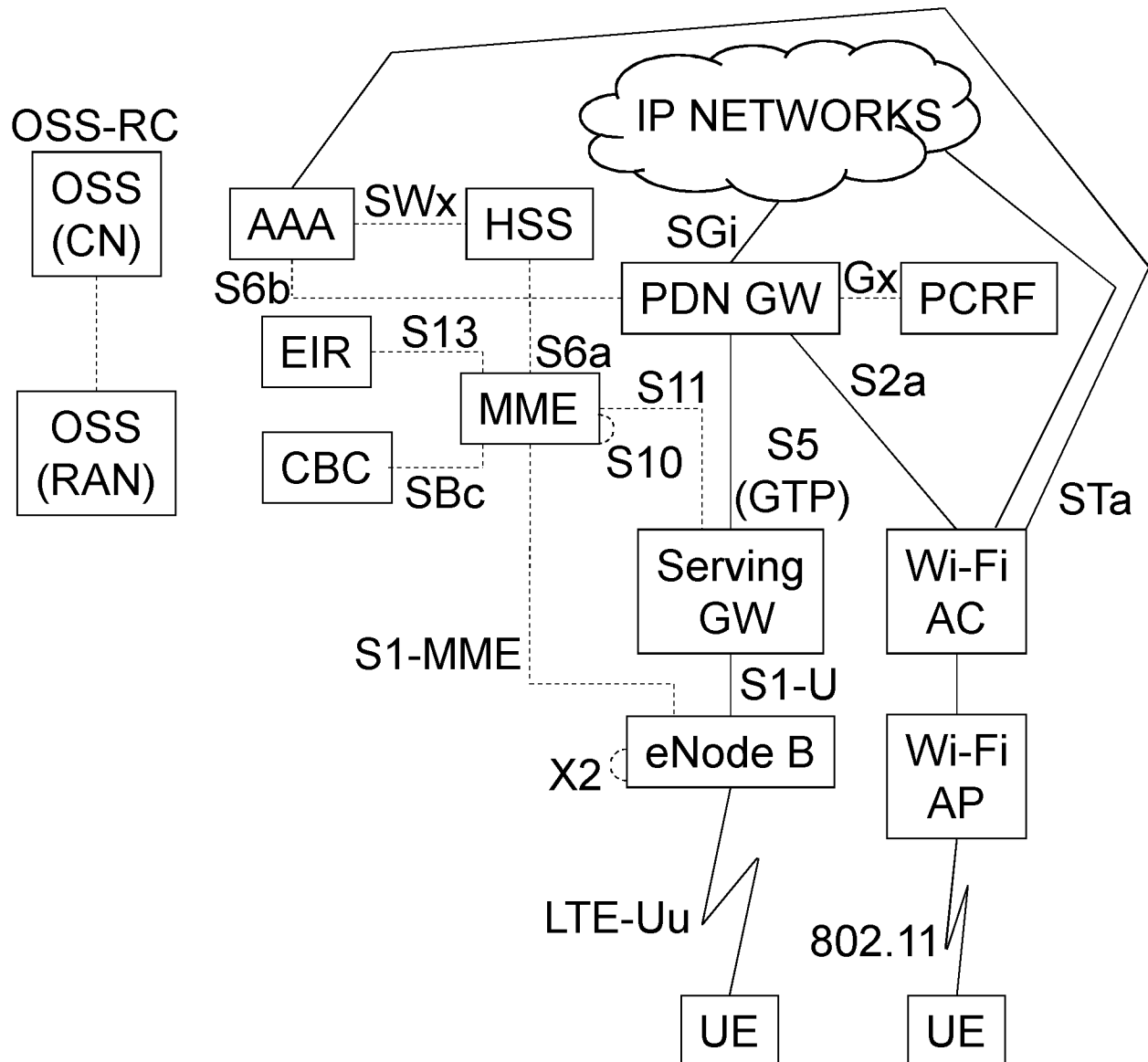
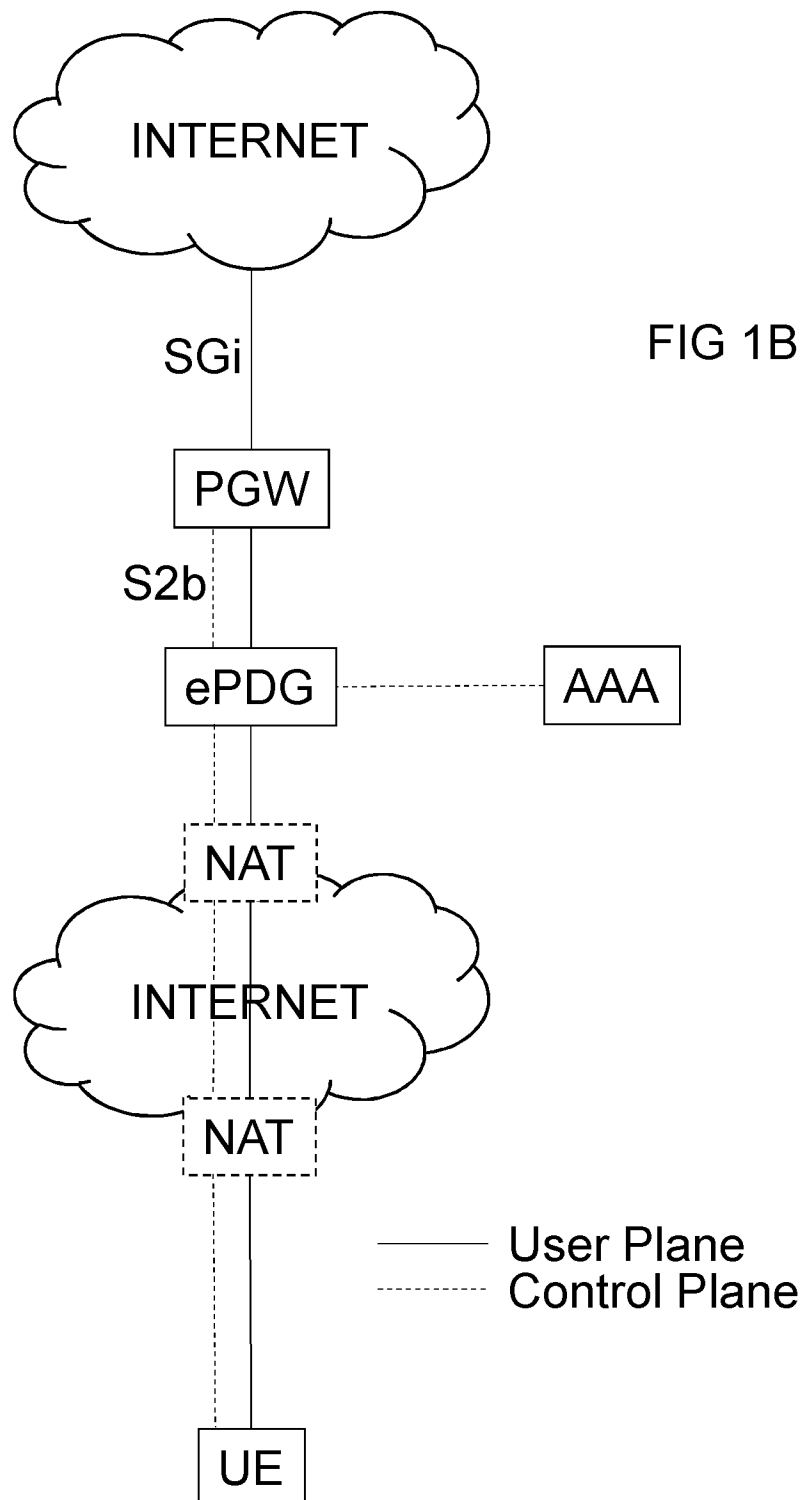


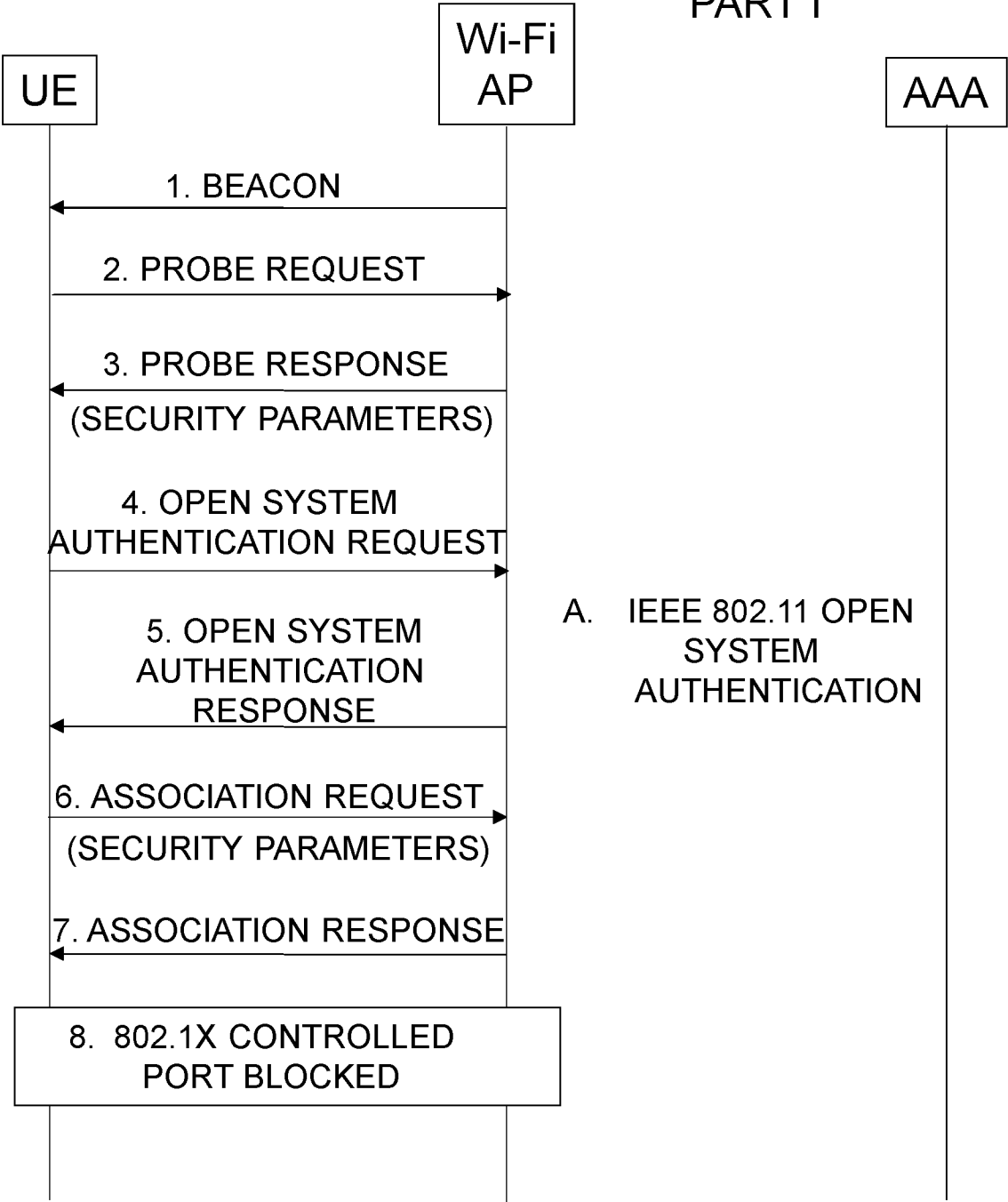
FIG 1A

2/21



3/21

FIG 2
PART I



TO FIG 2 PART II

FIG 2
PART II

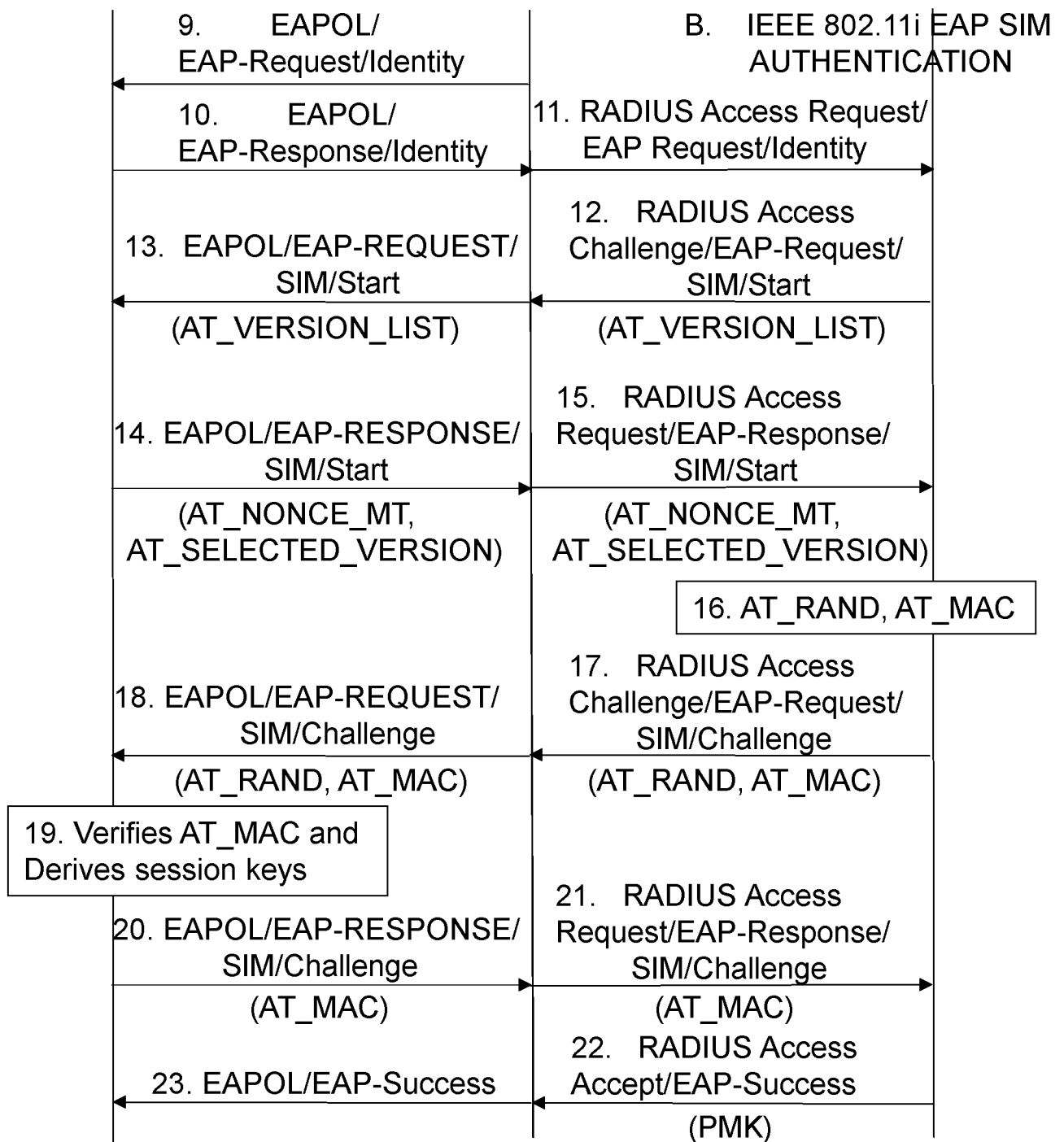
4/21

UE

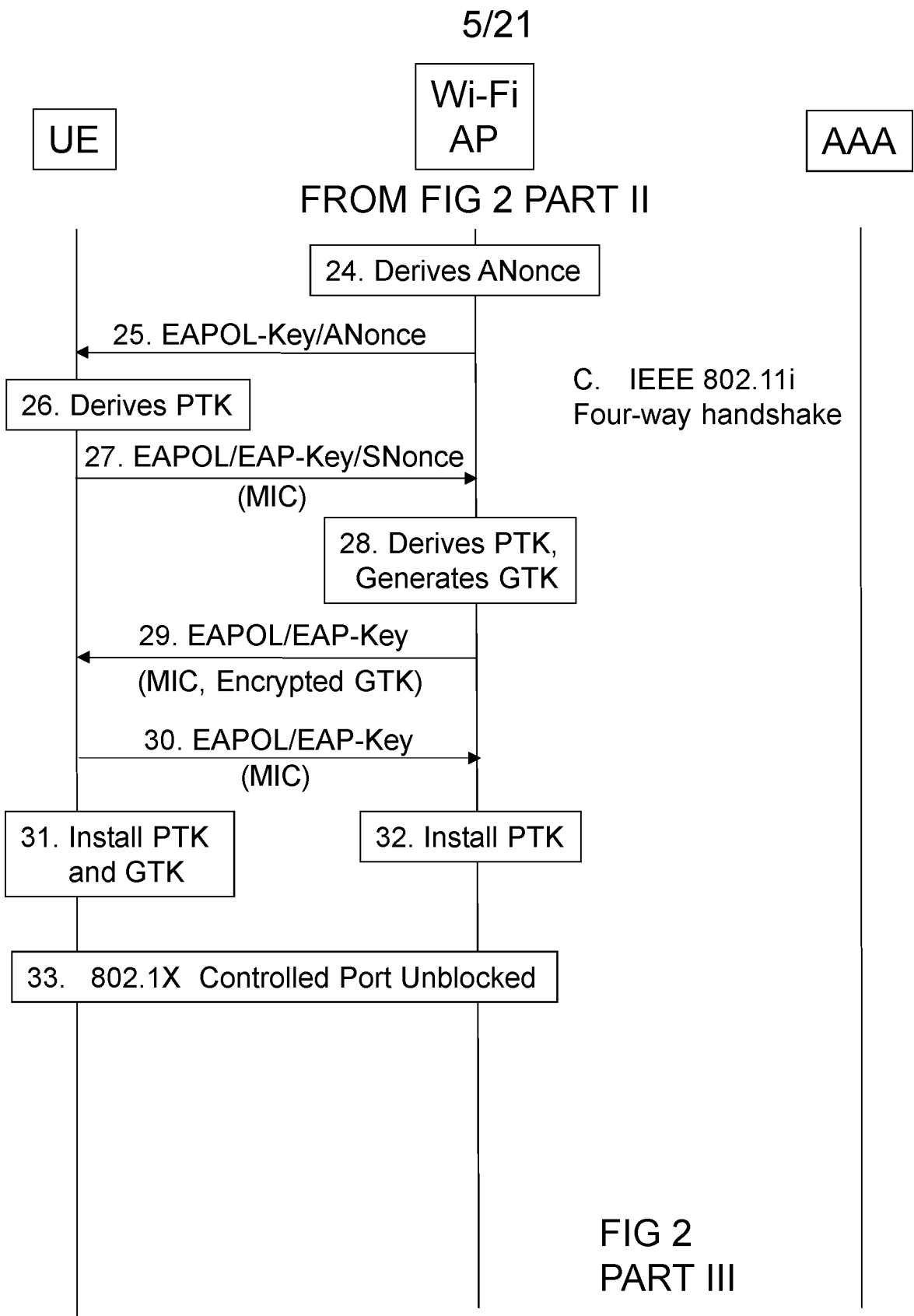
Wi-Fi
AP

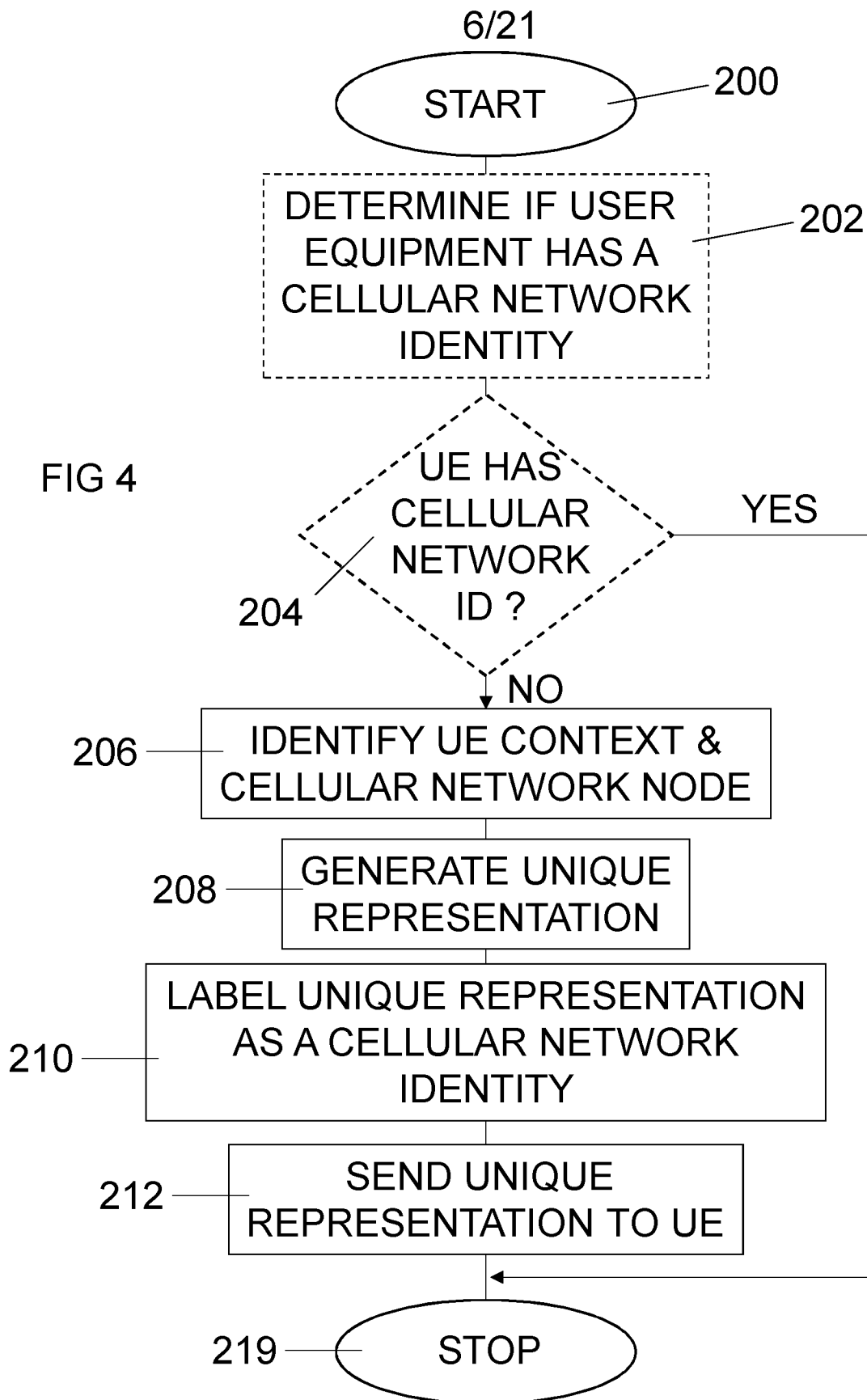
AAA

FROM FIG 2 PART I



TO FIG 2 PART III





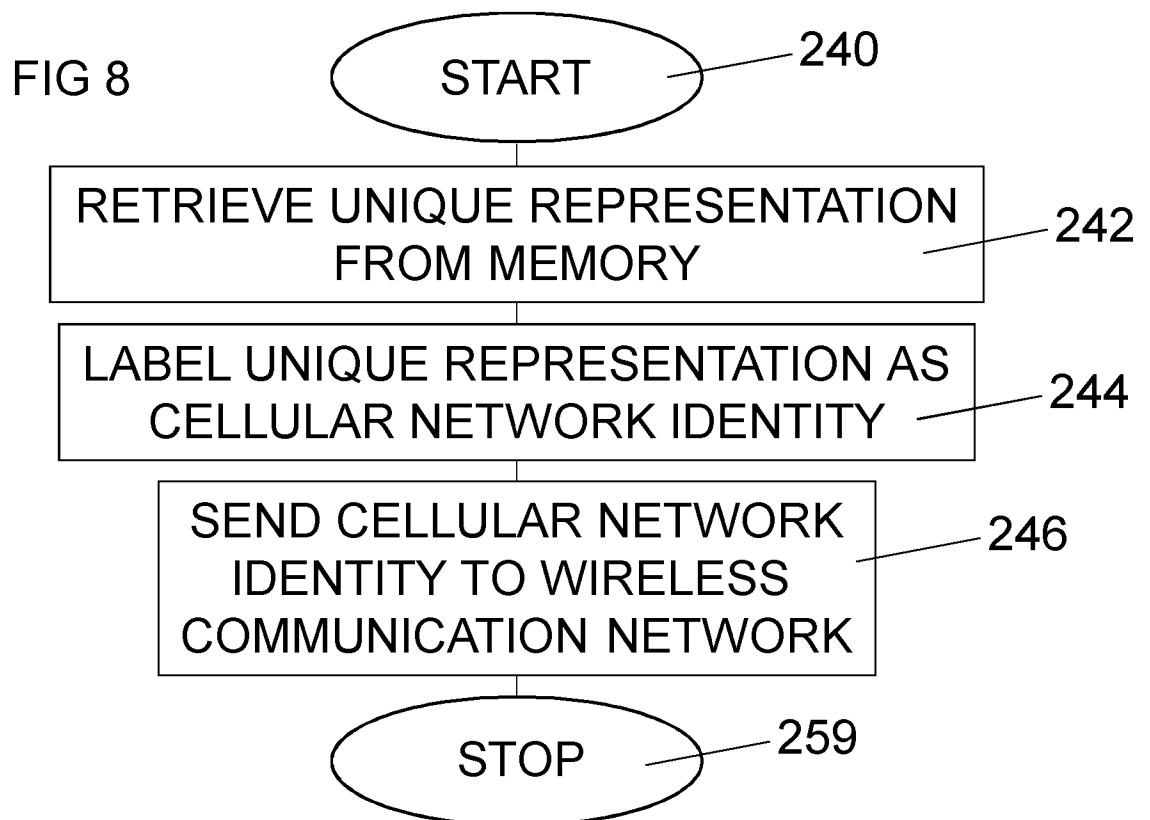
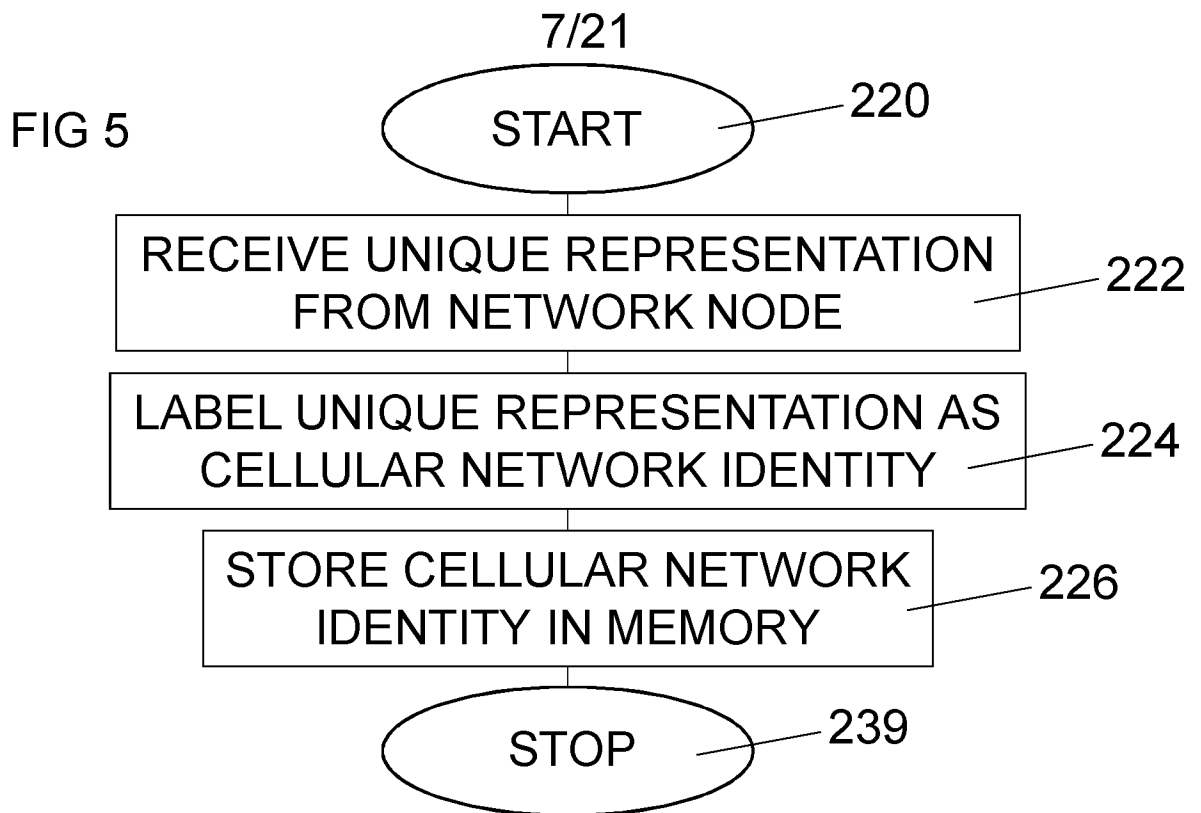
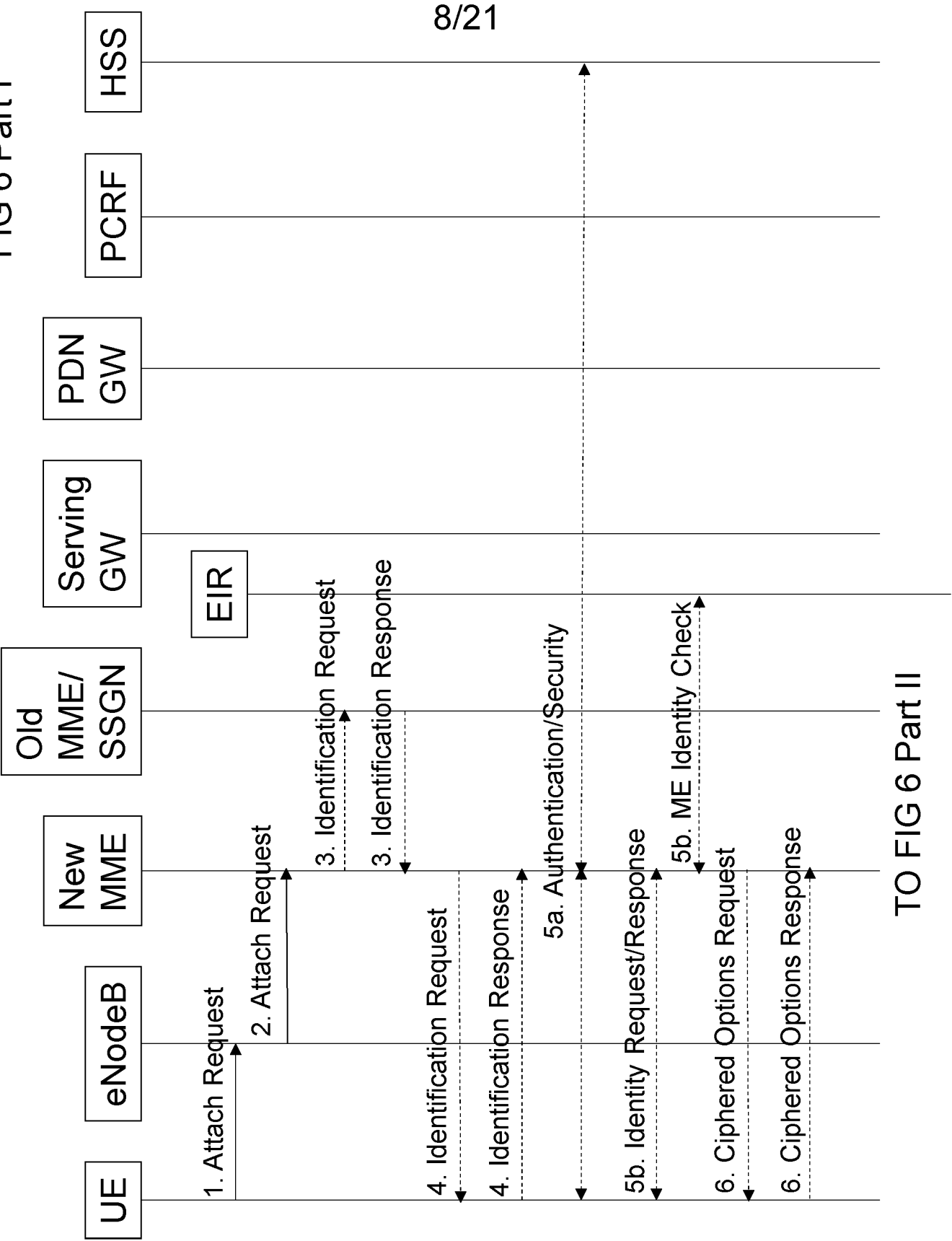
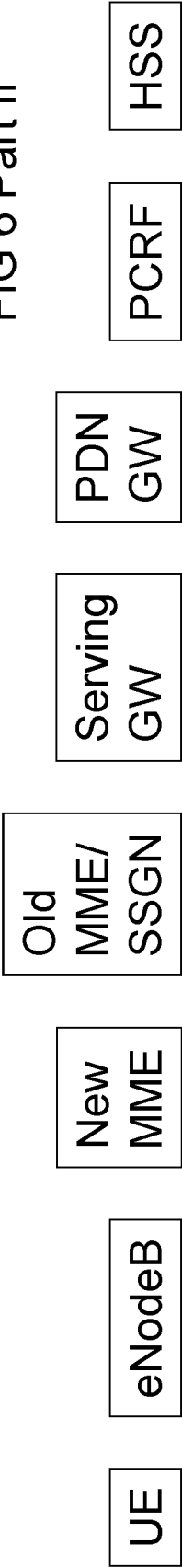


FIG 6 Part I

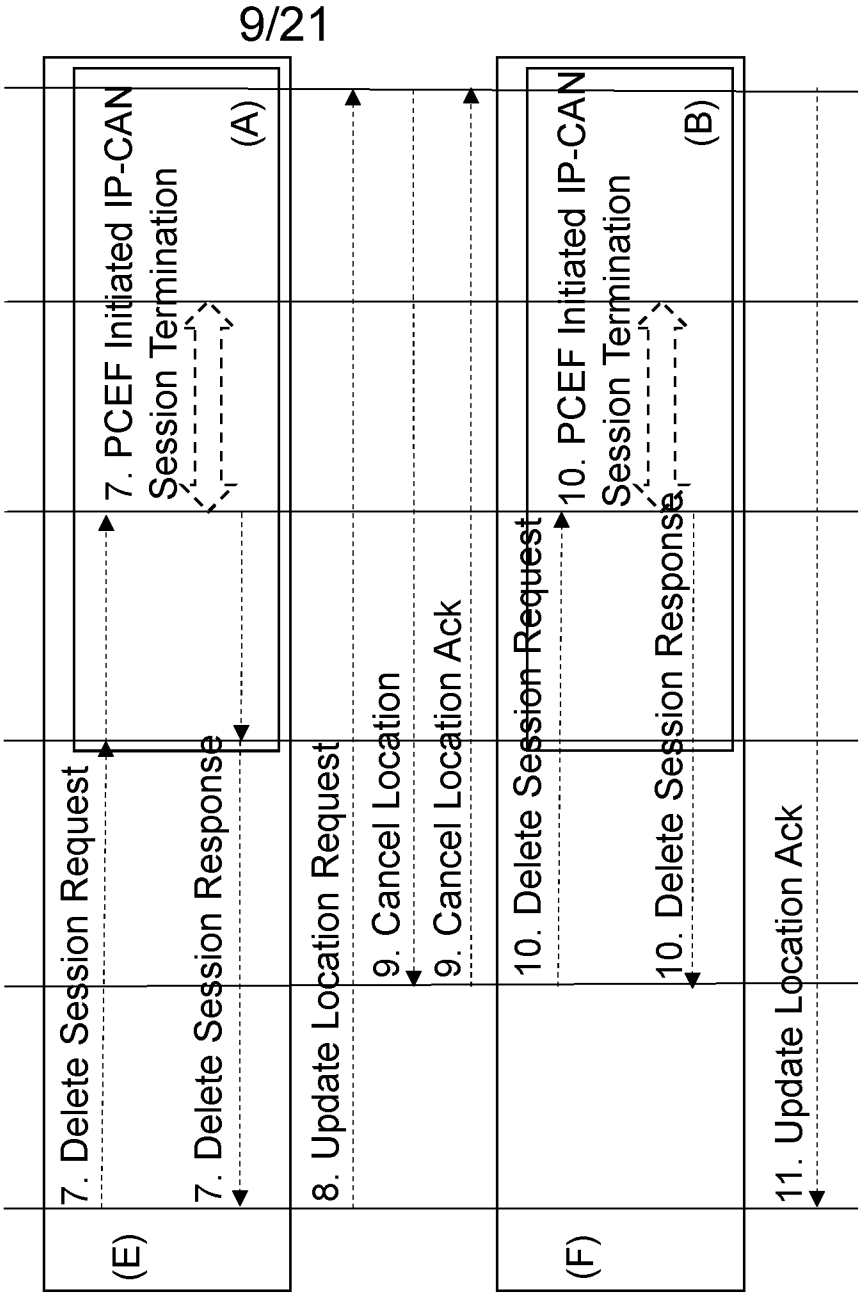


TO FIG 6 Part II

FIG 6 Part II

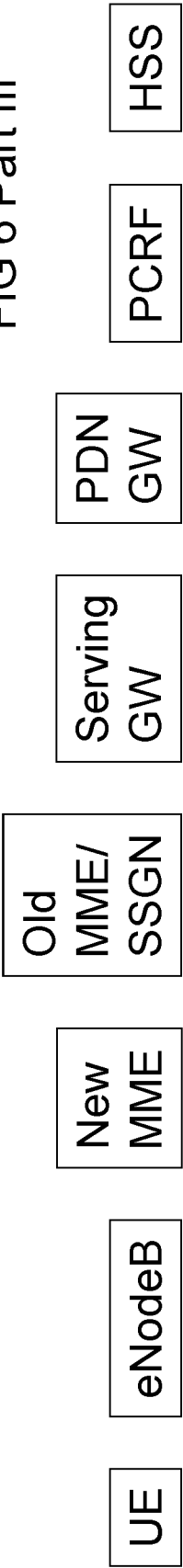


FROM FIG 6 Part I

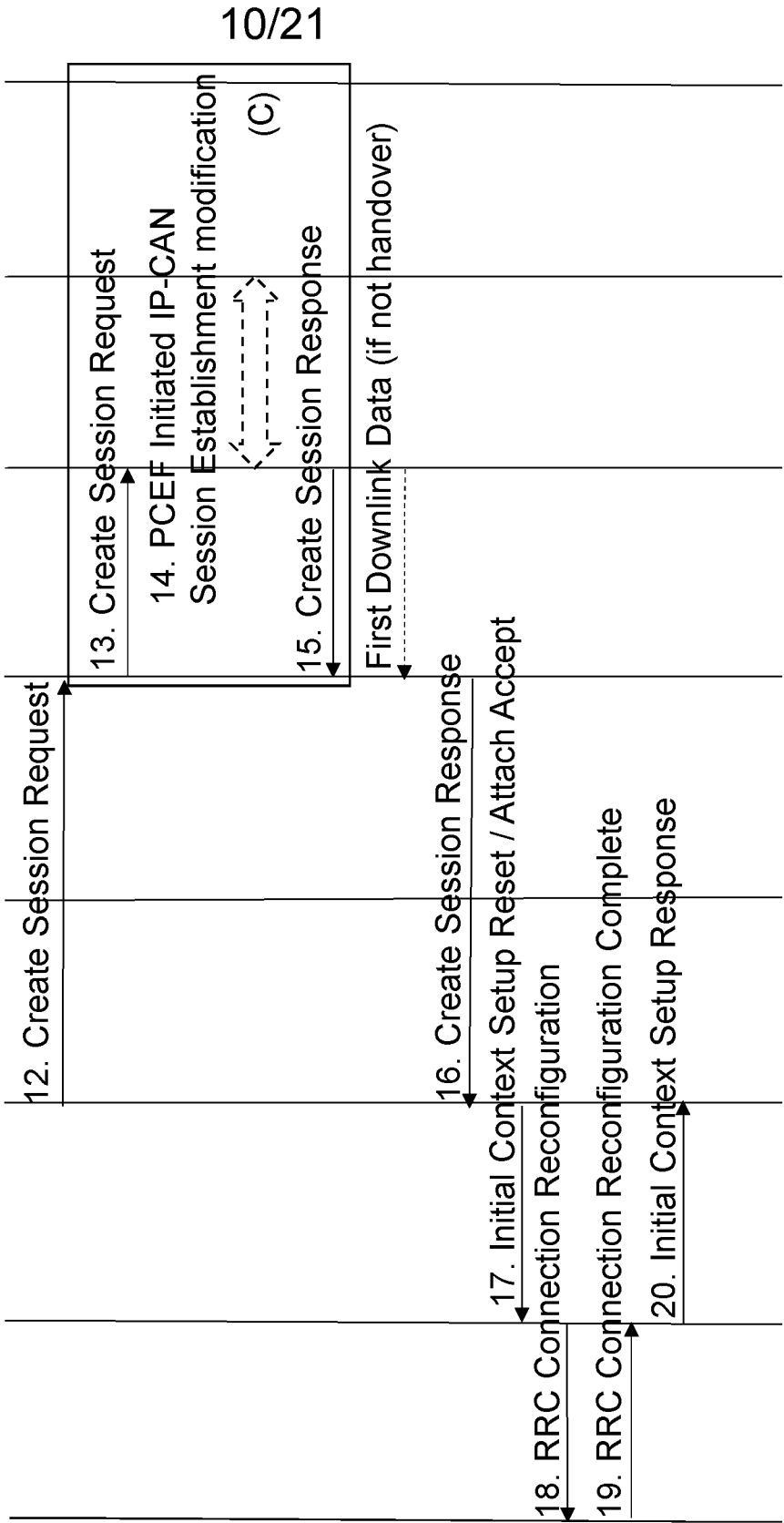


TO FIG 6 Part III

FIG 6 Part III

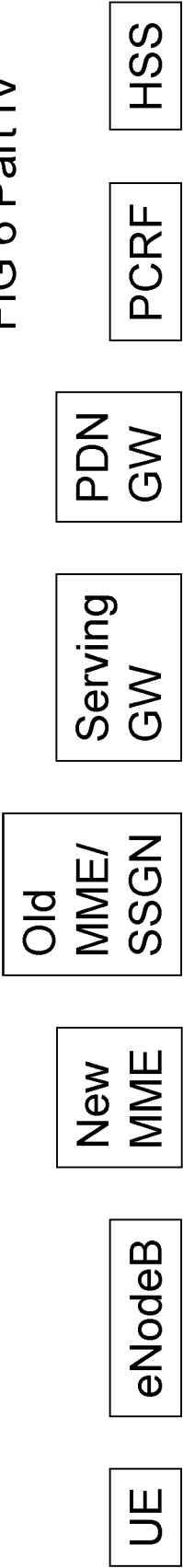


FROM FIG 6 Part II

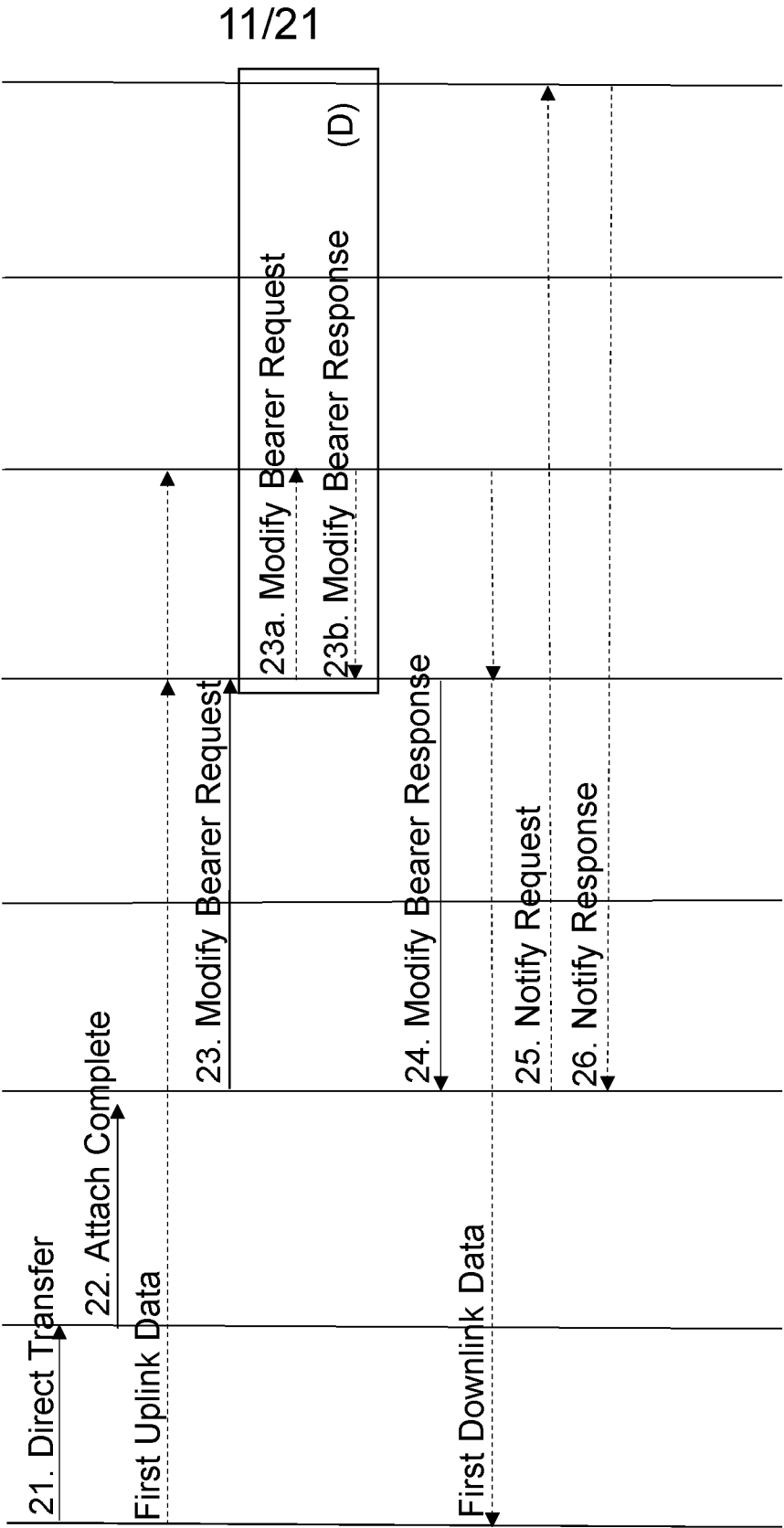


TO FIG 6 Part IV

FIG 6 Part IV



FROM FIG 6 Part III



12/21

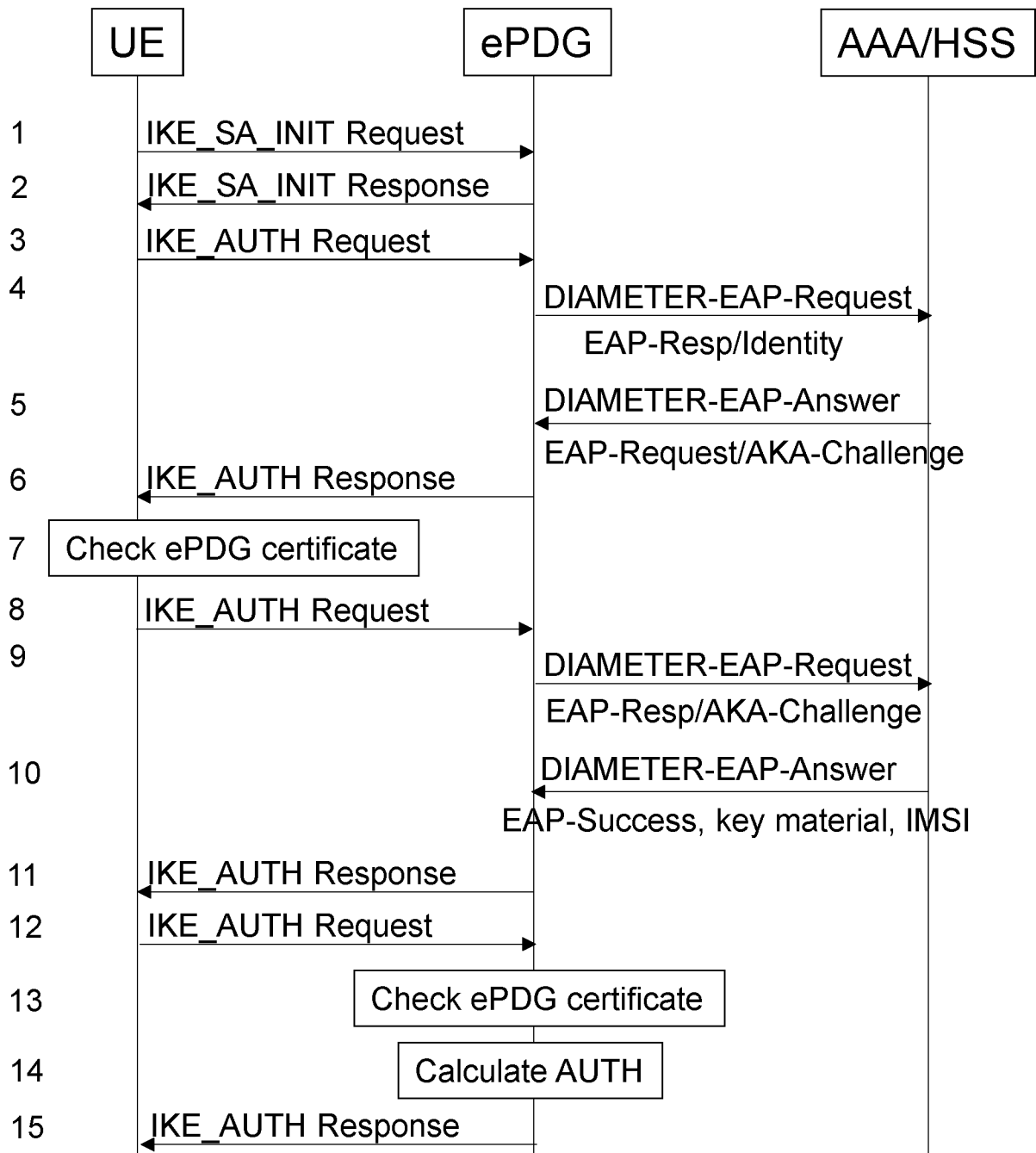
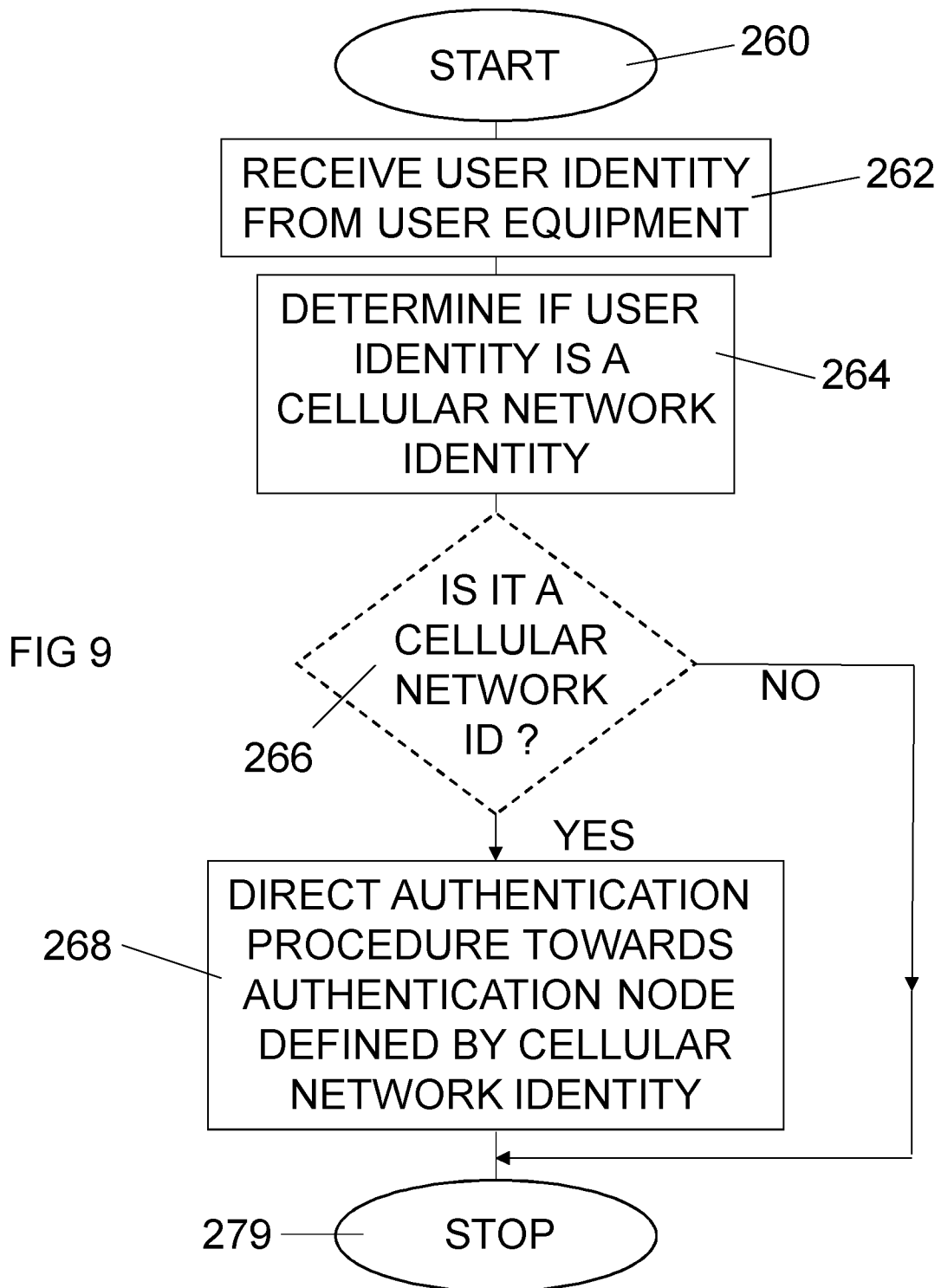


FIG 7

13/21



14/21

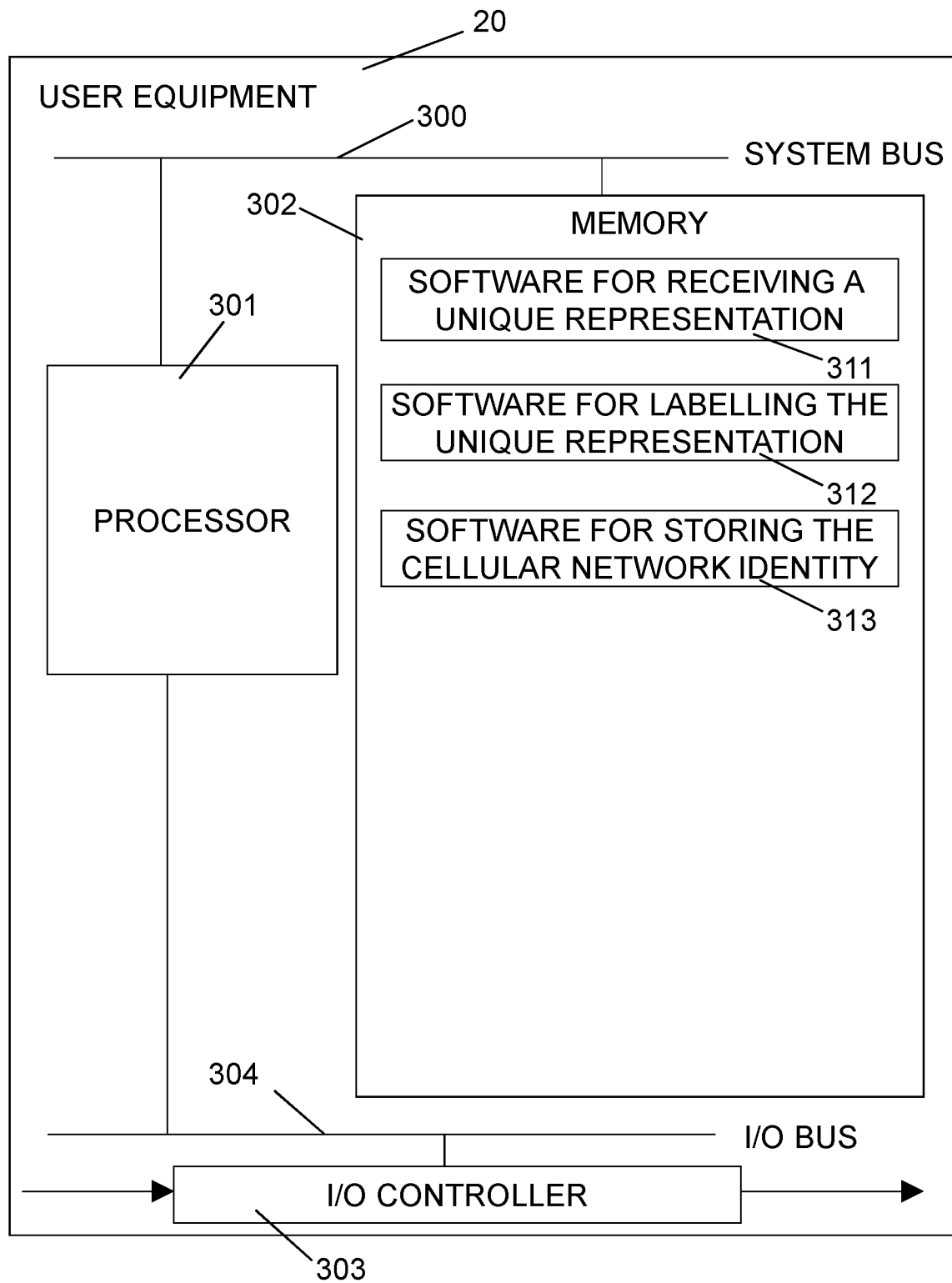


FIG 10

15/21

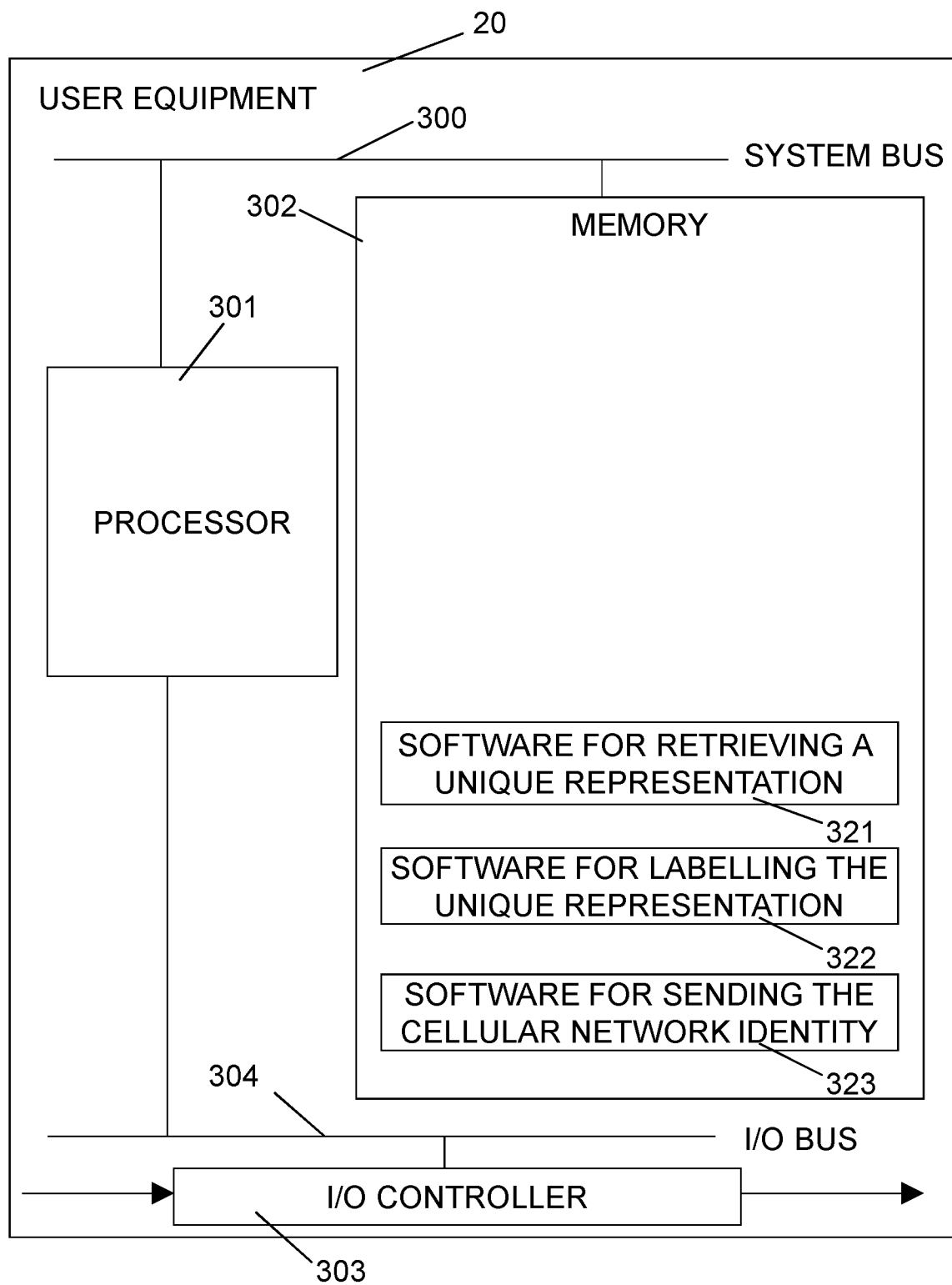


FIG 11

16/21

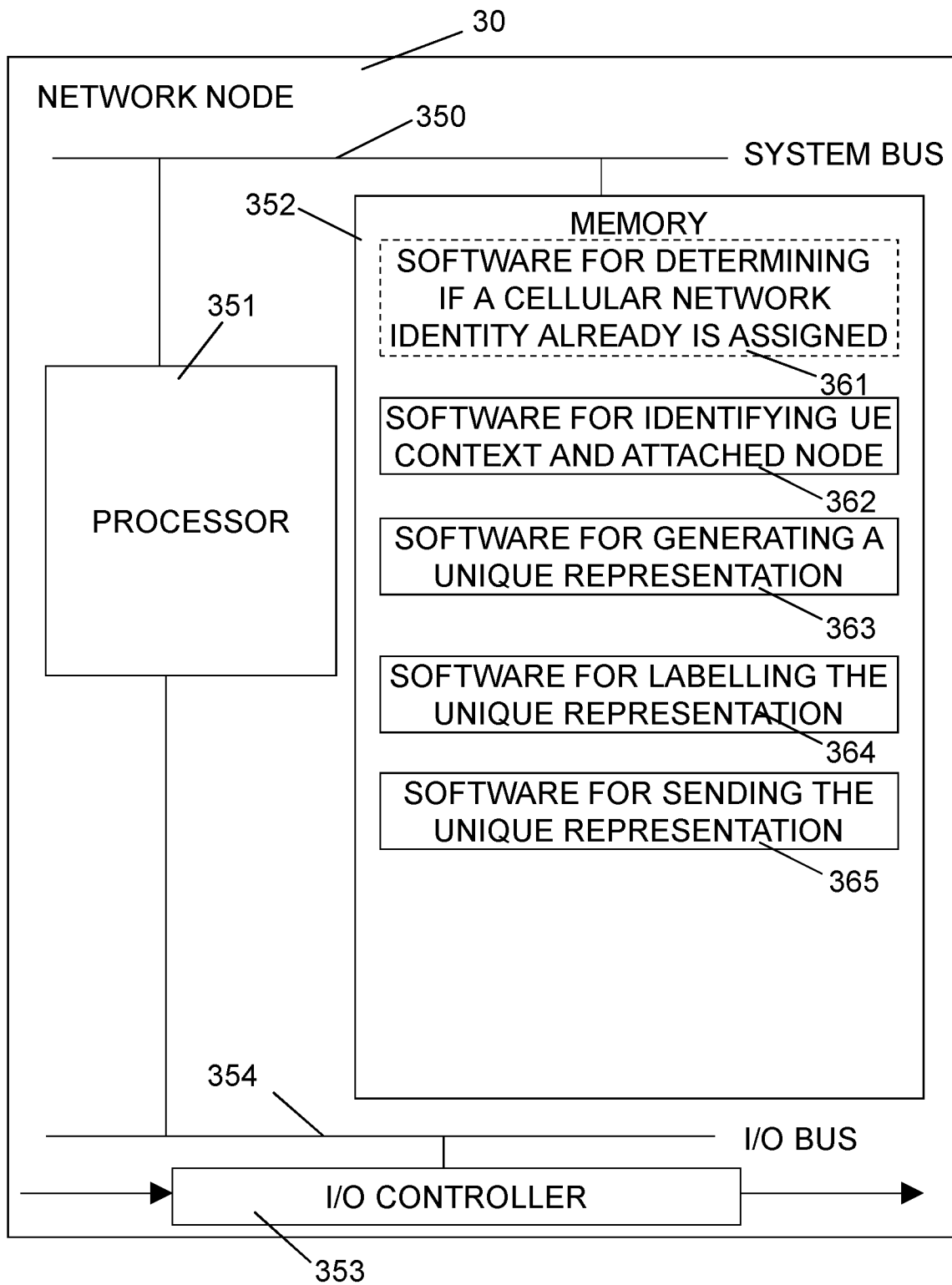


FIG 12

17/21

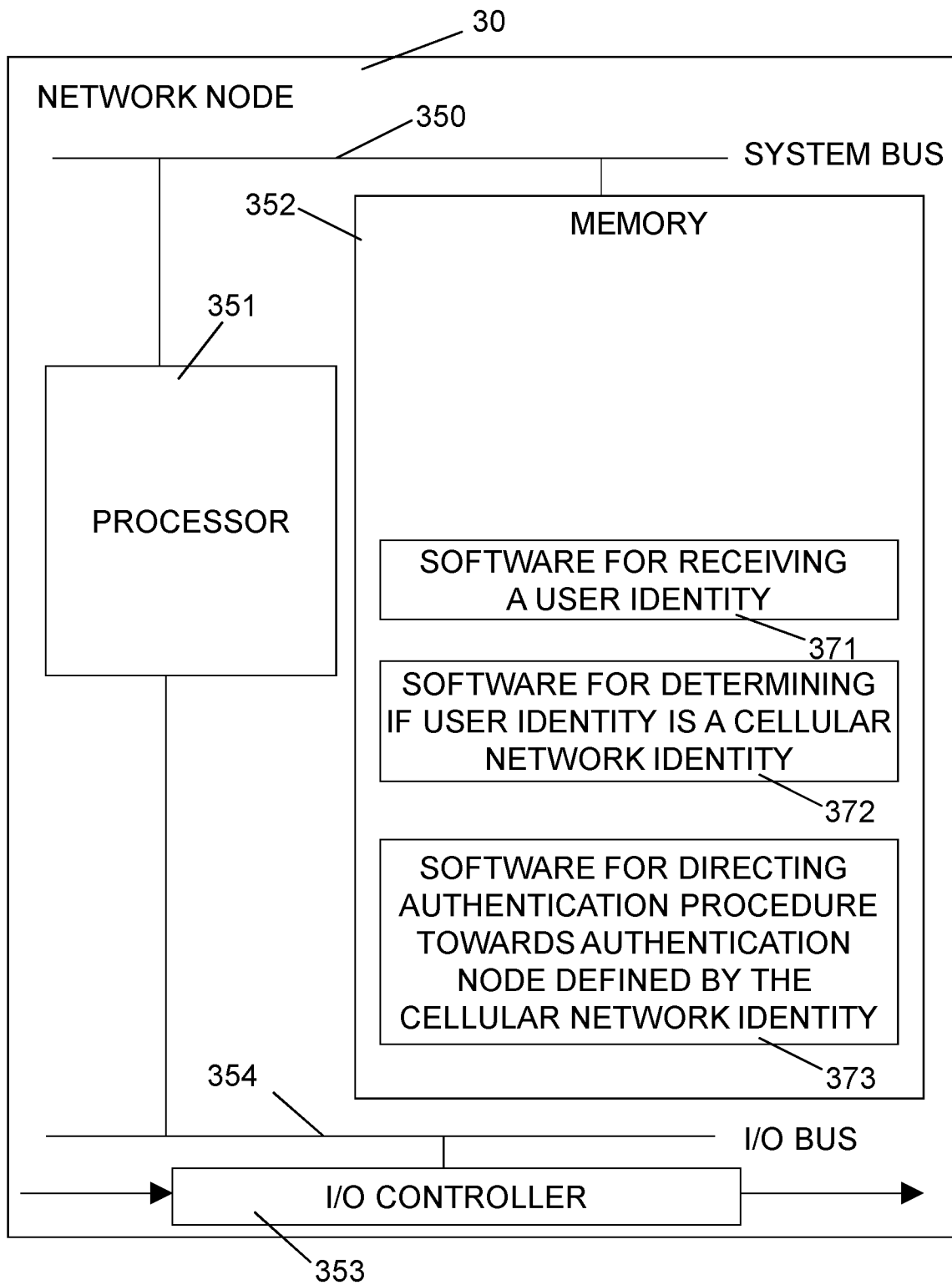


FIG 13

18/21

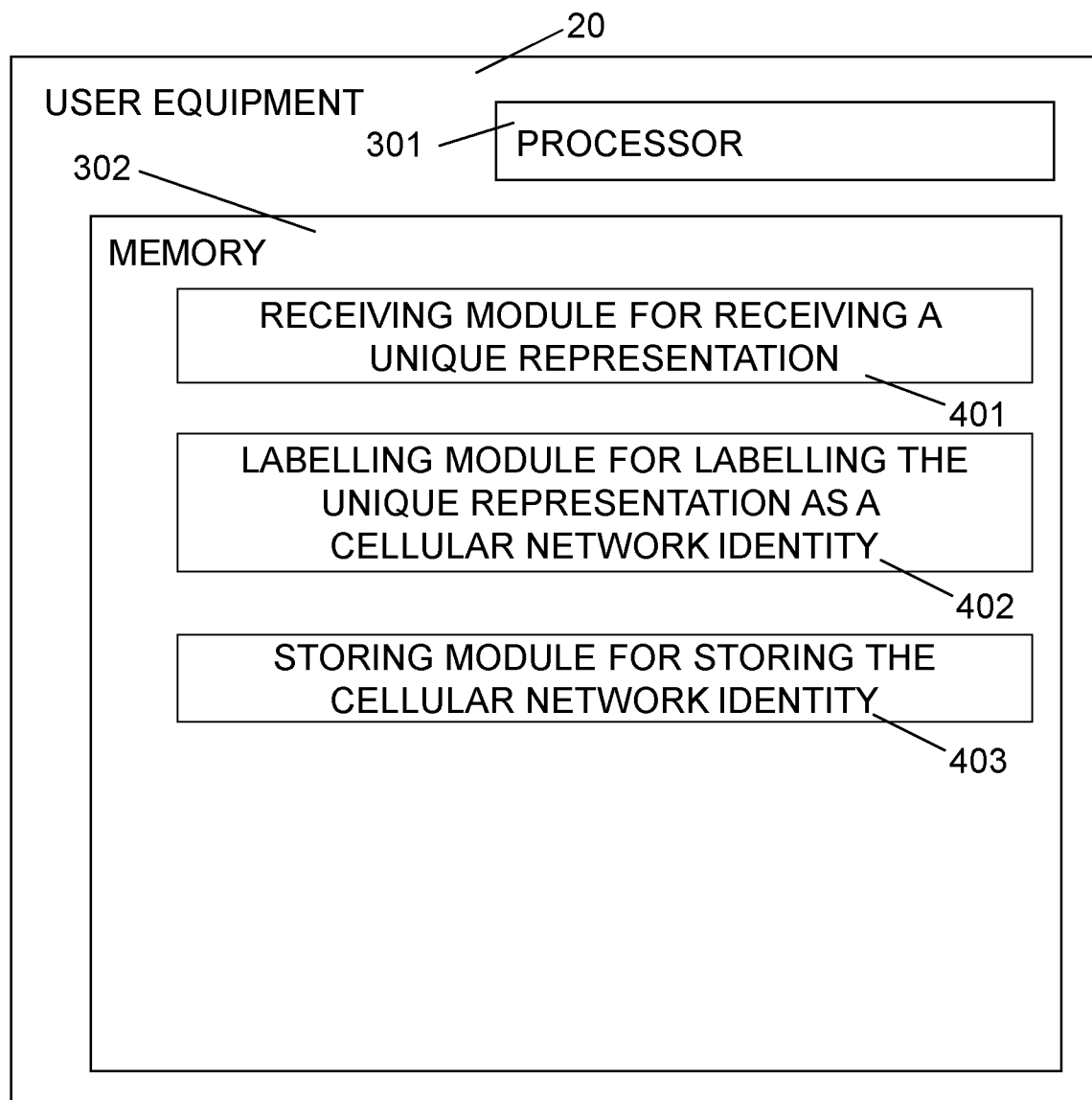


FIG 14

19/21

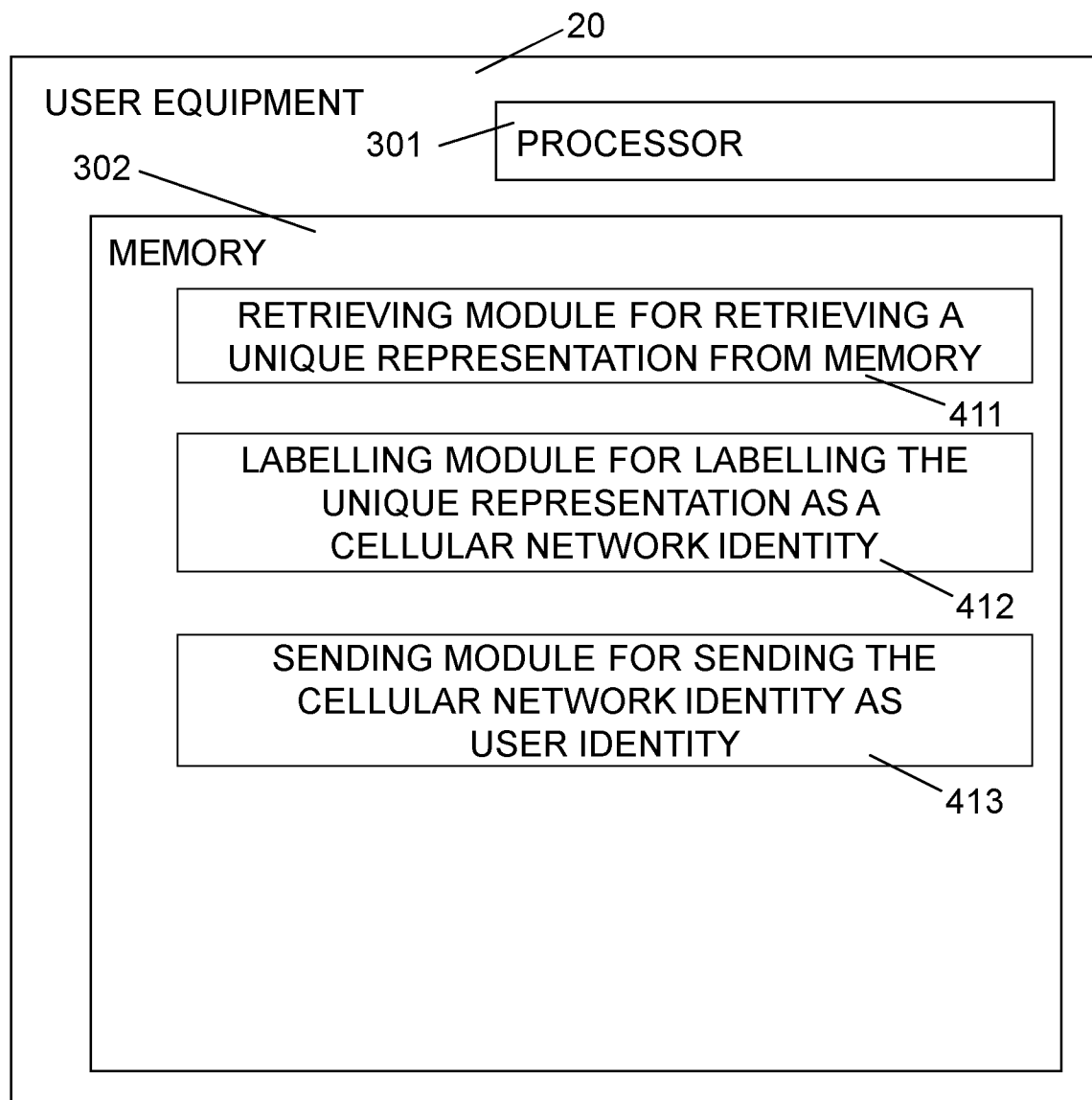


FIG 15

20/21

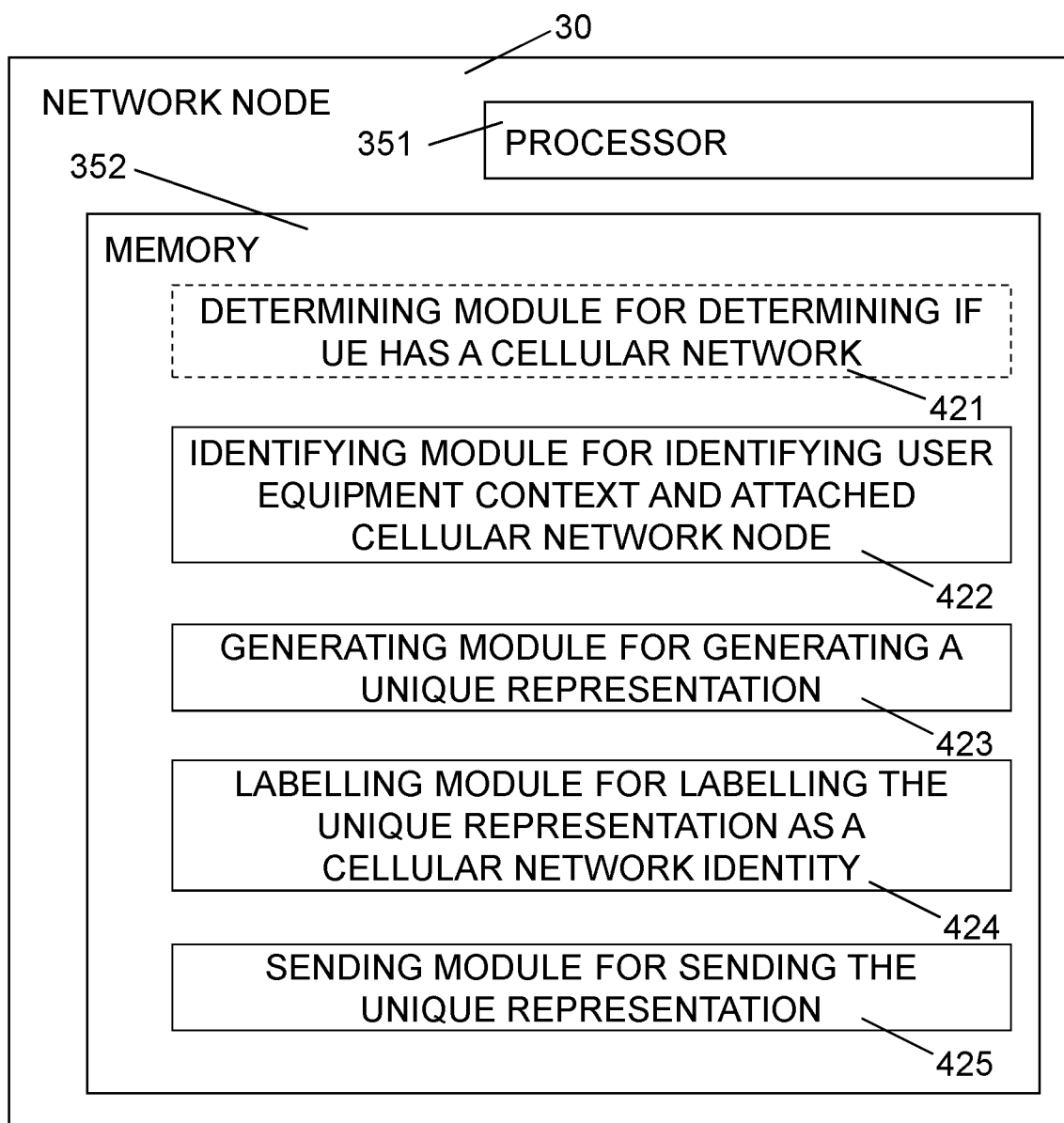


FIG 16

21/21

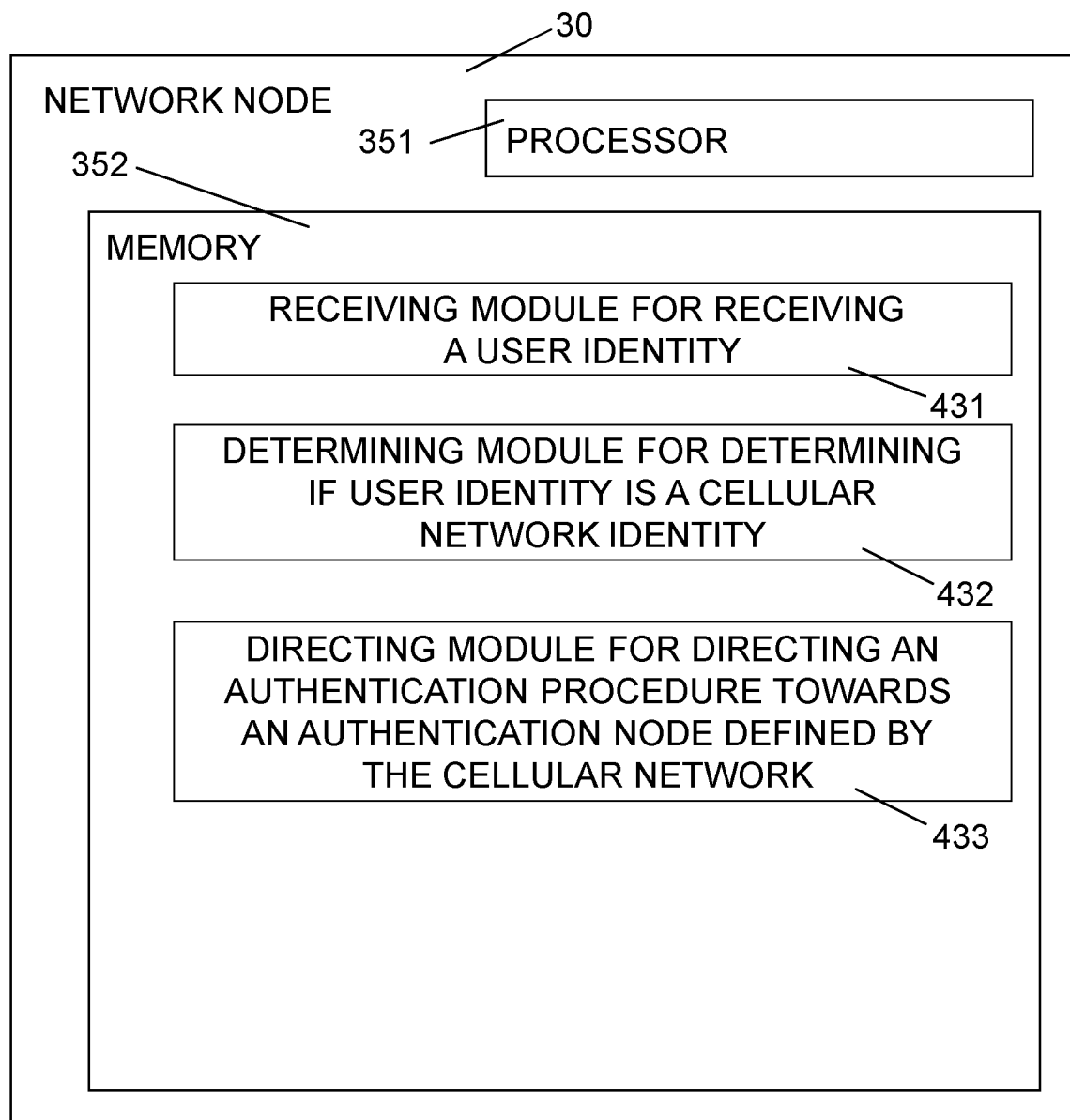


FIG 17

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE2014/051454

A. CLASSIFICATION OF SUBJECT MATTER

IPC: see extra sheet

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

SE, DK, FI, NO classes as above

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

EPO-Internal, PAJ, WPI data, COMPENDEX, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 2079253 A1 (PANASONIC CORP), 15 July 2009 (2009-07-15); abstract; pages 16-17 --	1-34
A	EP 1672945 A1 (SAMSUNG ELECTRONICS CO LTD), 21 June 2006 (2006-06-21); abstract --	1-34
A	US 20020191575 A1 (KALAVADE ASAWAREE ET AL), 19 December 2002 (2002-12-19); abstract --	1-34
A	US 20060046714 A1 (KALAVADE ASAWAREE), 2 March 2006 (2006-03-02); abstract -- -----	1-34

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:

“A” document defining the general state of the art which is not considered to be of particular relevance

“E” earlier application or patent but published on or after the international filing date

“L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

“O” document referring to an oral disclosure, use, exhibition or other means

“P” document published prior to the international filing date but later than the priority date claimed

“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

“&” document member of the same patent family

Date of the actual completion of the international search

09-10-2015

Date of mailing of the international search report

09-10-2015

Name and mailing address of the ISA/SE

Patent- och registreringsverket
Box 5055
S-102 42 STOCKHOLM
Facsimile No. + 46 8 666 02 86

Authorized officer

Ralf Boström

Telephone No. + 46 8 782 28 00

Continuation of: second sheet**International Patent Classification (IPC)***H04W 12/06* (2009.01)*H04W 36/14* (2009.01)*H04W 88/06* (2009.01)*H04W 92/02* (2009.01)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/SE2014/051454

EP	2079253 A1	15/07/2009	EP	2755423 A1	16/07/2014
			EP	2541987 B1	14/05/2014
			EP	2235985 B1	14/11/2012
			EP	2079261 A1	15/07/2009
			JP	2011509615 A	24/03/2011
			JP	5524863 B2	18/06/2014
			KR	20100109951 A	11/10/2010
			US	8457635 B2	04/06/2013
			US	20130324125 A1	05/12/2013
			US	20100323700 A1	23/12/2010
			US	8781474 B2	15/07/2014
			WO	2009087099 A1	16/07/2009
EP	1672945 A1	21/06/2006	KR	100762644 B1	01/10/2007
			KR	20060067263 A	19/06/2006
			US	20060128362 A1	15/06/2006
US	20020191575 A1	19/12/2002	CA	2450434 A1	27/12/2002
			EP	1405475 A1	07/04/2004
			US	7239632 B2	03/07/2007
			US	20080031211 A1	07/02/2008
			US	7782848 B2	24/08/2010
			WO	02103970 A1	27/12/2002
US	20060046714 A1	02/03/2006	CA	2591614 A1	09/03/2006
			EP	1784995 A2	16/05/2007
			US	7136651 B2	14/11/2006
			US	7818008 B2	19/10/2010
			US	20110009122 A1	13/01/2011
			US	20070060124 A1	15/03/2007
			WO	2006026726 A3	08/06/2006