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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
20 December 2018 (20.12.2018)

WIPO | PCT

(10) International Publication Number
WO 2018/231125 A1

(51) International Patent Classification:
H04W 12/06 (2009.01) *H04W 12/02* (2009.01)
H04W 48/18 (2009.01) *H04L 29/08* (2006.01)
H04W 4/00 (2018.01)

(21) International Application Number:
PCT/SE2018/050576

(22) International Filing Date:
04 June 2018 (04.06.2018)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
62/520,661 16 June 2017 (16.06.2017) US

(71) Applicant: **TELEFONAKTIEBOLAGET LM ERICSSON (PUBL)** [SE/SE]; 164 83 Stockholm (SE).

(72) Inventors: **OHLSSON, Oscar**; Malmgårdsvägen 30L, 116 38 Stockholm (SE). **HEDMAN, Peter**; Växjögatan 7E, 252 51 Helsingborg (SE). **PRAJWOL KUMAR, Prajwol**; Stupvägen 17, 191 42 Sollentuna (SE). **SCHLIWA-BERTLING, Paul**; Hjalmar Svenfelts väg 29 B, 590 71 Ljungsbro (SE).

(74) Agent: **AYOUB, Nabil**; Ericsson AB, Patent Unit Kista RAN 2, 164 80 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, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA,

(54) Title: NETWORK, NETWORK NODES, WIRELESS COMMUNICATION DEVICES AND METHOD THEREIN FOR HANDLING NETWORK SLICES IN A WIRELESS COMMUNICATION NETWORK

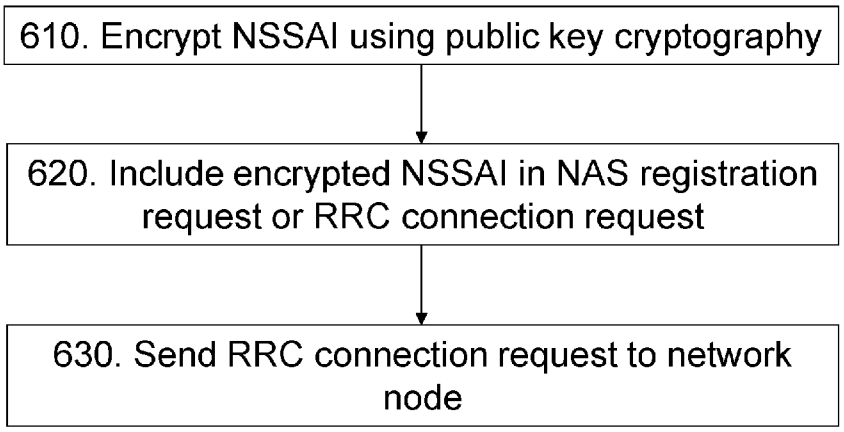

Fig. 6

(57) Abstract: A communication device, network node and methods therein in for handling network slices in a wireless communication network are disclosed. The communication device encrypts Network Slice Selection Assistance information, NSSAI, using public key cryptography and includes the encrypted NSSAI in a Non Access Stratum, NAS, registration request. Then the communication device sends a Radio Resource Control, RRC, request to the network node including the NAS registration request. The network node receives the RRC connection request from the communication device and selects a network function based on information in the RRC connection request. The network node forwards the NAS registration request to the network function and forwards to the communication device a NAS registration response received from the network function after the network function decrypting the NSSAI using a PLMN private

WO 2018/231125 A1

[Continued on next page]

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))*

— *in black and white; the international application as filed contained color or greyscale and is available for download from PATENTSCOPE*

NETWORK, NETWORK NODES, WIRELESS COMMUNICATION DEVICES AND METHOD THEREIN FOR HANDLING NETWORK SLICES IN A WIRELESS COMMUNICATION NETWORK

TECHNICAL FIELD

Embodiments herein relate to a network, a network node, a wireless communication device and methods therein. In particular, they relate to handle network slices during network registration for a wireless communication device in a wireless communication network.

BACKGROUND

In a typical wireless communication network, wireless devices, also known as wireless communication devices, mobile stations, stations (STA) and/or user equipments (UE), communicate via a Radio Access Network (RAN) to one or more core networks (CN). The RAN covers a geographical area which is divided into service areas or cell areas, which may also be referred to as a beam or a beam group, with each service area or cell area being served by a radio network node such as a radio access node e.g., a Wi-Fi access point or a radio base station (RBS), which in some networks may also be denoted, for example, a “NodeB” or “eNodeB” or “gNB”. A service area or cell area is a geographical area where radio coverage is provided by the radio network node. The radio network node communicates over an air interface operating on radio frequencies with the wireless device within a range of the radio network node.

A Universal Mobile Telecommunications System (UMTS) is a third generation (3G) telecommunication network, which evolved from the second generation (2G) Global System for Mobile Communications (GSM). Specifications for the Evolved Packet System (EPS), also called a Fourth Generation (4G) network, have been completed within the 3rd Generation Partnership Project (3GPP) and this work continues in the coming 3GPP releases, for example to specify a Fifth Generation (5G) network.

Network slicing is a new concept in 5G network to allow differentiated treatment depending on each customer requirements. Network slices may differ in supported features and network functions optimizations. The operator may also deploy multiple network slice instances delivering exactly the same features but for different groups of UEs, e.g. as they deliver a different committed service and/or because they may be dedicated to a customer.

A single UE can simultaneously be served by one or more network slices. A single UE may be served by at most 8 network slices at a time. The Access and Mobility Management Function (AMF) instance serving the UE logically belongs to each of the network slices serving the UE, i.e. this AMF instance is common to the network slices serving a UE.

The Network Slice Selection Assistance information (NSSAI) is a new identifier in the 5G system which is included at network registration in both Radio Resource Control (RRC) and Non Access Stratum (NAS) to allow the network to select the correct network slice(s). The NSSAI represents the network slices serving the UE and consists of one or more Single NSSAI (S-NSSAIs). Each S-NSSAI identifies a single network slice and is in turn comprised of two parts:

- Slice/Service type (SST) which identifies a type of slice e.g., enhanced Mobile BroadBand (eMBB) addressing human-centric use cases for access to multimedia content, services and data, or Ultra-reliable-low latency communications (URLLC) with strict requirements, especially in terms of latency and reliability.

- Slice Differentiator (SD) which distinguishes network slices of the same type e.g., two eMBB slices.

The NSSAI included at RRC level enables the RAN to select a suitable AMF, i.e. an AMF that supports the network slice(s) that the UE subscribes to. The NSSAI is provided both in the initial network registration i.e. “Attach” and in network registration triggered due to mobility when the UE enters a new registration area i.e. Tracking Area Update (TAU). The reason for providing NSSAI also in the latter case is because the new registration area may be served by a different AMF pool which requires a new AMF to be selected. The NSSAI is included in MSG5 of the RRC connection establishment which also carries the NAS registration request message. Once an AMF has been selected the CN uses the NSSAI provided at NAS level to select the CN part of the network slice.

If the RAN is unable to select an AMF based on the NSSAI or if no NSSAI is included, the request is routed to a default AMF. The default AMF can then choose to re-direct the UE to some more suitable AMF based on subscription information and information provided at NAS level. Thus the NSSAI included at RRC level can be regarded as an optimization to avoid unnecessary AMF re-directions.

For subsequent accesses where the UE remains within the same registration area e.g. service request and has already been assigned an AMF, no assistance information may need to be included in the RRC connection establishment. In this case the temporary UE Identity (Temp ID) assigned to the UE by the AMF during network

registration is sufficient for the RAN to locate the serving AMF. Temp ID is equivalent to System Architecture Evolution (SAE)-Temporary Mobile Subscriber Identity (S-TMSI) in Evolved Packet Core (EPC) and is included in MSG3 of the RRC connection establishment.

In some scenarios, the network slices a UE subscribes to are considered sensitive information e.g. access to public safety related slice(s), and network slice IDs should therefore preferably not be revealed. This is a problem in the current network slice selection procedure since the NSSAI is sent both in the NAS and RRC layers which are open over the air interface.

SUMMARY

Therefore it is an object of embodiments herein to provide an improved technique for handling network slices for a wireless communication device in a wireless communication network.

According to one aspect of embodiments herein, the object is achieved by a method performed in a wireless communication device for handling network slices in a wireless communication network. The wireless communication device encrypts Network Slice Selection Assistance information, NSSAI, using public key cryptography. Then includes the encrypted NSSAI in a Non Access Stratum, NAS, registration request. The wireless communication device further sends a Radio Resource Control, RRC, connection request to a network node including the NAS registration request.

According to one aspect of embodiments herein, the object is achieved by a wireless communication device for handling network slices in a wireless communication network. The wireless communication device is configured to encrypt Network Slice Selection Assistance information, NSSAI, using public key cryptography and include the encrypted NSSAI in a Non Access Stratum, NAS, registration request. The wireless communication device is further configured to send a Radio Resource Control, RRC, connection request to a network node including the NAS registration request.

According to one aspect of embodiments herein, the object is achieved by a method performed in a network node for handling network slices for a communication device in a wireless communication network. The wireless communication network comprises the network node in a Radio Access Network, RAN, and a network function in a core network, CN, of the wireless communication network. The network node receives a Radio

Resource Control, RRC, connection request from the wireless communication device and the RRC connection request comprises a NAS registration request including a Network Slice Selection Assistance information, NSSAI, encrypted using Public Land Mobile Network, PLMN, public key. The network node selects a network function based on information in the RRC connection request and forward the NAS registration request to the network function. The network node further forwards to the wireless communication device a NAS registration response received from the network function after the network function decrypting the NSSAI using a PLMN private key.

According to one aspect of embodiments herein, the object is achieved by a network node for handling network slices for a communication device in a wireless communication network. The wireless communication network comprises the network node in a Radio Access Network, RAN, and a network function in a core network, CN, of the wireless communication network. The network node is configured to receive a Radio Resource Control, RRC, connection request from the wireless communication device and the RRC connection request comprises a NAS registration request including a Network Slice Selection Assistance information, NSSAI, encrypted using Public Land Mobile Network, PLMN, public key. The network node is further configured to select a network function based on information in the RRC connection request and forward the NAS registration request to the network function. The network node is further configured to forward to the wireless communication device a NAS registration response received from the network function after the network function decrypting the NSSAI using a PLMN private key.

According to one aspect of embodiments herein, the object is achieved by a method performed in a wireless communication network for handling network slices for a communication device. The wireless communication network comprises a network node and a network function. The network node is in a Radio Access Network, RAN, and the network function is in a core network, CN, of the wireless communication network. The network node receives a Radio Resource Control, RRC, connection request from the communication device and the RRC connection request comprises a NAS registration request including a Network Slice Selection Assistance information, NSSAI, encrypted using Public Land Mobile Network, PLMN, public key. The network node selects a network function based on information provided in the RRC connection request. The network nod forwards to the network function the NAS registration request. The network function decrypts the encrypted NSSAI using a PLMN private key. The network node

receives from the network function a NAS registration response. The network node sends to the communication device the NAS registration response.

According embodiments herein, to avoid revealing information about the network slices the UE subscribes to at network registration, the NSSAI included in NAS is encrypted using public key cryptography, e.g. the Home Public Land Mobile Network's (HPLMN's) or Registered PLMN's (RPLMN) public key.

The NSSAI included in RRC may be replaced with a new identifier, e.g. an AMF selection ID, which is only used for AMF routing.

The NSSAI included at NAS level is encrypted at least for the initial network registration when no NAS context is available and NAS security has not yet been activated. At subsequent, e.g. mobility triggered, network registrations no additional encryption is required as NAS security will be activated at this point.

The AMF selection ID may be sent in clear text in RRC, but since it does not identify the individual network slices, less information is revealed than if NSSAI is included. An additional benefit of the AMF selection ID is that it may be shorter than NSSAI which reduces the size of the RRC message.

Alternatively, the NSSAI in NAS may be encrypted using the HPLMN or RPLMN's public key, in the same way as above, and the NSSAI in RRC may be encrypted using a RAN public key. This requires though that the RAN public key can be securely distributed to the UE, e.g. by being signed with a root key and broadcasted in system information or provided over NAS protected using NAS security.

In a further alternative, the NSSAI in NAS may be encrypted using the HPLMN or RPLMN's public key, in the same way as above, and no identifier is included in RRC. As no information is included in RRC, the RAN selects a default AMF which then potentially re-directs the UE based on the encrypted NSSAI provided in NAS.

In yet another alternative, the NSSAI in NAS and in RRC may both be encrypted using the HPLMN or RPLMN's public key. This requires that the HPLMN or RPLMN's public key is provided by the AMF(s) to the RAN in a secure manner, e.g. by using IP Security (IPsec) during the establishment of the RAN/CN or New core network to N2 (NG-C/N2) interface. In a roaming scenario, in case the HPLMN's public key is used, the UE needs additionally to provide in RRC the HPLMN identity to assist the RAN in selection of the right public key to decrypt the NSSAI. For the non-roaming case and in shared RAN scenario, the RAN selects the public key based on UE's indication of the selected PLMN.

The embodiments herein improve user privacy in network slicing by avoiding revealing information about which network slices the UE subscribes to at network

registration. This is done by either encrypting the network slice identifier using public key cryptography, replacing the identifier with a less specific identifier revealing less information, or omitting the identifier and relying on re-direction, or a combination of these mechanisms.

BRIEF DESCRIPTION OF THE DRAWINGS

Examples of embodiments herein are described in more detail with reference to attached drawings in which:

Figure 1 is a schematic block diagram depicting embodiments of a wireless communication network;

Figure 2 is a signaling diagram illustrating a first embodiment of handling network slices in a wireless communication network;

Figure 3 is a signaling diagram illustrating a second embodiment of handling network slices in a wireless communication network;

Figure 4 is a signaling diagram illustrating a third embodiment of handling network slices in a wireless communication network;

Figure 5 is a signaling diagram illustrating a fourth embodiment of handling network slices in a wireless communication network;

Figure 6 is flowchart illustrating a method performed in a wireless communication device according to embodiments herein;

Figure 7 is flowchart illustrating a method performed in a network node according to embodiments herein;

Figure 8 is flowchart illustrating a method performed in a wireless communication network according to embodiments herein; and

Figure 9 is a schematic block diagram illustrating one embodiment of an UE,a network node or a second network node.

DETAILED DESCRIPTION

Please note that the terms “UE” “user equipment” and wireless communication device are used interchangeably in this document.

Embodiments herein relate to a wireless communication networks in general. **Figure 1** is a schematic overview depicting **a wireless communication network 100**. The wireless communication network 100 may be a wireless communications network

comprising one or more RANs and one or more CNs. The wireless communication network 100 may use a number of different technologies, such as Wi-Fi, Long Term Evolution (LTE), LTE-Advanced, 5G, Wideband Code Division Multiple Access (WCDMA), Global System for Mobile communications/enhanced Data rate for GSM Evolution (GSM/EDGE), Worldwide Interoperability for Microwave Access (WiMax), or Ultra Mobile Broadband (UMB), just to mention a few possible implementations. Embodiments herein relate to recent technology trends that are of particular interest in a 5G context, however, embodiments are also applicable in further development of the existing wireless communication systems such as e.g. WCDMA and LTE.

In the wireless communication network 100, wireless communication devices e.g. **a user equipment 130** such as a mobile station, a non-access point (non-AP) STA, a STA, or a wireless terminal, communicates via one or more Access Networks (AN), e.g. RAN, to one or more core networks (CN). It should be understood by the skilled in the art that "wireless communication device" is a non-limiting term which means any terminal, wireless communication terminal, user equipment, Machine Type Communication (MTC) device, Device to Device (D2D) terminal, or node e.g. smart phone, laptop, mobile phone, sensor, relay, mobile tablets or even a small base station communicating within a cell. The terms user equipment 130, UE, UE 130 and wireless communication device 130 are used interchangeable herein.

Network nodes operate in the wireless communication network 100 such as **a first network node 111** and a **second network node 112**. The first network node 111 provides radio coverage over a geographical area, **a service area 11**, which may also be referred to as a beam or a beam group where the group of beams is covering the service area of a first radio access technology (RAT), such as 5G, LTE, Wi-Fi or similar. The second network node 112 provides radio coverage over a geographical area, **a service area 12**, which may also be referred to as a beam or a beam group where the group of beams is covering the service area of a first radio access technology (RAT), such as 5G, LTE, Wi-Fi or similar.

The first and second network nodes 111 and 112 may be a transmission and reception point e.g. a radio access network node such as a Wireless Local Area Network (WLAN) access point or an Access Point Station (AP STA), an access controller, a base station, e.g. a radio base station such as a NodeB, a gNB, an evolved Node B (eNB, eNode B), a base transceiver station, a radio remote unit, an Access Point Base Station, a base station router, a transmission arrangement of a radio base station, a stand-alone

access point or any other network unit capable of communicating with a wireless device within the service area served by the respective first and second network nodes 111 and 112 depending e.g. on the first radio access technology and terminology used. The first and second network nodes 111 and 112 may be referred to as a serving radio network node and communicates with the wireless device 130 with Downlink (DL) transmissions to the wireless device 130 and Uplink (UL) transmissions from the wireless device 130.

The wireless communication network 100 further comprises a CN 140 where one or more network functions, e.g. an AMF, are included.

Example Embodiments will be described in the following.

Embodiment 1: NSSAI in NAS encrypted using PLMN public key, NSSAI in RRC replaced with new identifier.

Figure 2 illustrates a signal flow chart of this embodiment in the wireless communication network 100.

In this embodiment, the NSSAI included in NAS is encrypted with the HPLMN or RPLMN's public key and the NSSAI included in RRC is replaced with a new identifier which is only used for AMF routing.

The HPLMN or RPLMN's public key used to encrypt the NSSAI included in NAS is assumed to be pre-configured by the HPLMN. Alternatively, the HPLMN or RPLMN's public key can be delivered to the UE 130 via e.g. system information broadcast. In this case some form of PKI is needed to securely distribute the public key. If the HPLMN public key used for encryption and the UE 130 is roaming, i.e. HPLMN ≠ RPLMN, the RPLMN may need assistance from the HPLMN to decrypt the NSSAI unless it has access to the HPLMN private key.

The AMF selection ID included in RRC level can either be pre-configured in the UE or configured over NAS in the initial registration. In the latter case no AMF selection ID is included in the initial registration which means the RAN selects a default AMF.

The message flow for the network registration is shown in Figure 2 and described as following steps:

Step 201: The UE 130 establishes the RRC connection establishment and includes the AMF selection ID and the NAS registration request. The NAS registration request in turn includes the NSSAI which the UE has encrypted using the HPLMN or RPLMN's public key. In case the network registration is triggered due to mobility, i.e. UE entering a new registration area, the UE will also provide the identity of the old AMF and its Temp ID in order for the new AMF to be able to retrieve the UE NAS context from the old AMF.

This is similar to Tracking Area Update in LTE where the UE provides GUMMEI and S-TMSI to allow the UE context to be retrieved from the old MME.

Step 202: The RAN routes the NAS registration to an AMF based on the AMF selection ID. If no AMF selection ID is provided the RAN selects a default AMF.

Step 203: The AMF decrypts the NSSAI in the NAS registration request using the HPLMN or RPLMN's private key and selects the CN part of the network slice(s). If the AMF does not support the network slices indicated in the NSSAI the UE is re-directed to another AMF.

Step 204: In case the UE 130 is already registered to the network, the AMF retrieves the UE NAS context from the old AMF based on the Old AMF ID and Temp ID.

Step 205: For the initial network registration, the AMF identifies the UE and establishes NAS security.

Step 206: Provided the UE 130 is allowed to register to the network, the AMF replies with a NAS registration setup.

Step 207: The acknowledges the NAS registration setup by sending the NAS registration setup complete.

Step 208: The RRC connection is released by the RAN.

Note that the NSSAI included at NAS level only needs to be encrypted using the public key in the initial registration when no NAS context exists and NAS security has not yet been activated. At subsequent registrations, NAS security is activated and the NAS layer encryption ensures the confidentiality of the NSSAI.

Embodiment 2: NSSAI in NAS encrypted using PLMN public key and NSSAI in RRC encrypted using RAN public key.

In this embodiment, the NSSAI is included in both RRC and NAS at network registration. The NSSAI in NAS is encrypted using the HPLMN or RPLMN public key, in the same way as the previous embodiment, and the NSSAI in RRC is encrypted using a RAN public key.

The message flow for the network registration is the same as in the first embodiment except that the NSSAI encrypted with the RAN public key is included in the first step 201 instead of the AMF selection ID. This is shown in **Figure 3**. The gNB 111 decrypts the NSSAI using the RAN private key and uses it to route the NAS registration request to a suitable AMF.

The RAN public key can either be specific for each gNB or common for all gNBs in the RAN. In general, using individual keys is more secure as it provides security compartmentalization, i.e. the compromise of one gNB does not impact other gNBs.

The RAN public key can either be delivered in the broadcasted system information or configured over NAS in the initial registration. In the latter case no NSSAI is included in RRC in the initial registration which means the RAN selects a default AMF.

As a potential optimization, the NSSAI in NAS can be omitted and instead the RAN can forward the NSSAI included in RRC to the AMF. This approach requires though that the NSSAI is always provided in RRC, including the initial network registration.

Embodiment 3: NSSAI in NAS encrypted using PLMN public key, no NSSAI in RRC.

In this embodiment the NSSAI is included only in NAS at network registration and no information is included in the RRC level.

The message flow for the network registration is the same as in the first embodiment except that the AMF selection ID is omitted in the first step 201. This is shown in **Figure 4**. As no routing information is included in RRC, the AMF always selects a default AMF. The default AMF then potentially re-directs the UE 130 based on the encrypted NSSAI provided in NAS.

Compared to the previous embodiment, this embodiment is simpler but potentially results in more AMF re-directions which increases latency and the amount of RAN/CN signaling.

Embodiment 4: NSSAI in NAS and RRC both encrypted using PLMN public key.

In this embodiment, the NSSAI is included in both RRC and NAS at network registration. The NSSAI in NAS and RRC are both encrypted using the HPLMN or RPLMN public key.

The message flow for the network registration is the same as in the first embodiment except that the NSSAI encrypted with the HPLMN or RPLMN public key is included in the first step 201 instead of the AMF selection ID. This is shown in **Figure 5**. The gNB 111 decrypts the NSSAI using the HPLMN or RPLMN private key and uses it to route the NAS registration request to a suitable AMF.

In a roaming scenario, in case the HPLMN's public key is used, the UE needs additionally to provide in RRC, the HPLMN identity to assist the RAN in selection of the

right public key to decrypt the NSSAI. For the non-roaming case and in shared RAN scenario, the RAN selects the public key based on UE's indication of the selected PLMN.

Embodiments herein improve user privacy in network slicing by avoiding revealing information about which network slices the UE subscribes to during network registration. This is done by either encrypting the network slice identifier using public key cryptography, replacing the identifier with a less specific identifier revealing less information, omitting the identifier and relying on re-direction, or a combination of these mechanisms as described above.

According to these embodiments, a method performed in the communication device 130 for handling network slices in the wireless communication network (100) is now described with reference to Figure 6. The method comprises the following actions, which may be performed in any suitable order.

Action 610

The communication device 130 encrypts Network Slice Selection Assistance information, NSSAI, using public key cryptography. The encryption may be performed using Public Land Mobile Network, PLMN, public key.

According some embodiments herein, the communication device 130 may encrypt Network Slice Selection Assistance information, NSSAI, using Radio Access Network, RAN, public key. The RAN public key may be specific for each network node or common for all network nodes in the RAN.

Action 620

The communication device 130 includes the encrypted NSSAI in a Non Access Stratum, NAS, registration request.

According some embodiments herein, the communication device 130 may include the encrypted NSSAI in the RRC connection request.

According some embodiments herein, the communication device 130 may include an AMF selection identifier in the RRC connection request. The AMF selection identifier may be pre-configured in the communication device 130 or configured over a NAS in an initial registration.

Action 630

The communication device 130 sends a Radio Resource Control, RRC, connection request to a network node including the NAS registration request.

According to the embodiments herein, a method performed in a network node 111 for handling network slices for a communication device 130 in a wireless communication network 100 will be described with reference to Figure 7. The wireless communication network 100 comprises the network node in a Radio Access Network, RAN, and a network function, e.g. AMF, in a CN. The method comprises following actions, which may be performed in any suitable order.

Action 710

The network node 111 receives a RRC connection request from the communication device 130. The RRC connection request comprises a NAS registration request including a NSSAI encrypted using PLMN public key.

Action 720

The network node 111 selects a network function based on information in the RRC connection request.

According to some embodiments, the network function is selected based on a AMF selection identifier provided in the RRC connection request.

According to some embodiments, the network function is selected based on a RAN public key encrypted NSSAI provided in the RRC connection request.

According to some embodiments, the network function is selected based on a PLMN public key encrypted NSSAI provided in the RRC connection request.

According to some embodiments, the network function is selected based on a default AMF if no AMF selection identifier is included in the RRC connection request.

Action 730

The network node 111 forwards the NAS registration request to the network function.

Action 740

The network node 111 forwards to the communication device 130 a NAS registration response received from the network function after the network function decrypting the NSSAI using a PLMN private key.

According to the embodiments herein, a method performed in a wireless communication network 100 for handling network slices for a communication device 130

is now described with reference to Figure 8. The wireless communication network 100 comprises a network node in a RAN and a network function in a CN of the wireless communication network 100. The method comprises following actions, which may be performed in any suitable order.

Action 810

The network node 111 receives a RRC connection request from the communication device 130. The RRC connection request comprises a NAS registration request including a NSSAI encrypted using PLMN public key.

Action 820

The network node 111 selects a network function based on information provided in the RRC connection request.

Action 830

The network node forwards to the network function the NAS registration request.

Action 840

The network function decrypts the encrypted NSSAI using a PLMN private key.

Action 850

The network node 111 receives from the network function a NAS registration response.

Action 860

The network node 111 sends to the communication device 130 the NAS registration response.

To perform the method in the UE 130 or in the network node 111/112, the UE 130 or the network node 111/112 comprises modules as shown in **Figure 9**. The UE/network node 130/111/112 comprises a **receiving module 910**, **a transmitting module 920, a determining module 930, a processing module 940, a memory 950** etc.

The communication device 130 is configured to, by means of e.g. the determining module 930 being configured to, encrypt NSSAI using public key cryptography. The encryption may be performed using Public Land Mobile Network, PLMN, public key.

According some embodiments herein, the communication device 130 may be configured to encrypt NSSAI using RAN public key. The RAN public key may be specific for each network node or common for all network nodes in the RAN.

The communication device 130 may be further configured to include the encrypted NSSAI in a NAS registration request.

According some embodiments herein, the communication device 130 may be further configured to include the encrypted NSSAI in the RRC connection request.

According some embodiments herein, the communication device 130 may be further configured to include an AMF selection identifier in the RRC connection request. The AMF selection identifier may be pre-configured in the communication device 130 or configured over a NAS in an initial registration.

The communication device 130 is further configured to, by means of e.g. transmitting model 920 being configured to, send a RRC connection request to a network node including the NAS registration request.

The network node 111 is configured to, by means of e.g. receiving model 910 being configured to, receive a RRC connection request from the communication device 130. The RRC connection request comprises a NAS registration request including a NSSAI encrypted using PLMN public key.

The network node 111 is configured to, by means of e.g. the determining module 930 being configured to, select a network function based on information in the RRC connection request.

According to some embodiments, the network function is selected based on a AMF selection identifier provided in the RRC connection request.

According to some embodiments, the network function is selected based on a RAN public key encrypted NSSAI provided in the RRC connection request.

According to some embodiments, the network function is selected based on a PLMN public key encrypted NSSAI provided in the RRC connection request.

According to some embodiments, the network function is selected based on a default AMF if no AMF selection identifier is included in the RRC connection request.

The network node 111 is further configured to, by means of e.g. transmitting module 920 being configured to, forward the NAS registration request to the network function.

The network node 111 is further configured to, by means of e.g. transmitting module 920 being configured to,forward to the communication device 130 a NAS registration response received from the network function after the network function decrypting the NSSAI using a PLMN private key.

Those skilled in the art will appreciate that the receiving unit 910, the determining unit 930 and the transmitting unit 920 described above in the UE/network node 130/111/112 may be referred to one circuit/unit, a combination of analog and digital circuits, one or more processors configured with software and/or firmware and/or any other digital hardware performing the function of each circuit/unit. One or more of these processors, the combination of analog and digital circuits as well as the other digital hardware, may be included in a single application-specific integrated circuitry (ASIC), or several processors and various analog/digital hardware may be distributed among several separate components, whether individually packaged or assembled into a system-on-a-chip (SoC).

The embodiments herein for handling network slices in the wireless communication network 100 performed in the wireless communication device/network node 130/111/112 may be implemented through one or more processors, such as the processing unit 940 together with computer program code for performing the functions and actions of the embodiments herein. The program code mentioned above may also be provided as a computer program product, for instance in the form of a **data carrier 980** carrying computer **program code 970** for performing the embodiments herein when being loaded into the communication device/network node. One such carrier may be in the form of a CD ROM disc. It is however feasible with other data carriers such as a memory stick. The computer program code 970 may furthermore be provided as pure program code on the cloud and downloaded to the communication device/network node 130/111/112.

The memory 950 in communication device/network node 130/111/112 may comprise one or more memory units and may be arranged to be used to store information, look up tables, historic lists, data, configurations and applications to perform the methods herein when being executed in communication device/network node 130/111/112.

As used herein, the term “processing module” may refer to a processing circuit, a processing unit, a processor, an Application Specific integrated Circuit (ASIC), a Field-Programmable Gate Array (FPGA) or the like. As an example, a processor, an ASIC, an FPGA or the like may comprise one or more processor kernels. In some examples, the processing module may be embodied by a software module or hardware module. Any such module may be a determining means, estimating means, capturing means, associating means, comparing means, identification means, selecting means, receiving

means, transmitting means or the like as disclosed herein. As an example, the expression "means" may be a module, such as a determining module, selecting module, etc.

As used herein, the expression "configured to" may mean that a processing circuit is configured to, or adapted to, by means of software configuration and/or hardware configuration, perform one or more of the actions described herein.

As used herein, the term "memory" may refer to a hard disk, a magnetic storage medium, a portable computer diskette or disc, flash memory, random access memory (RAM) or the like. Furthermore, the term "memory" may refer to an internal register memory of a processor or the like.

As used herein, the term "computer readable medium" may be a Universal Serial Bus (USB) memory, a DVD-disc, a Blu-ray disc, a software module that is received as a stream of data, a Flash memory, a hard drive, a memory card, such as a MemoryStick, a Multimedia Card (MMC), etc.

As used herein, the term "computer readable code units" may be text of a computer program, parts of or an entire binary file representing a computer program in a compiled format or anything there between.

As used herein, the terms "number", "value" may be any kind of digit, such as binary, real, imaginary or rational number or the like. Moreover, "number", "value" may be one or more characters, such as a letter or a string of letters. "number", "value" may also be represented by a bit string.

As used herein, the expression "in some embodiments" has been used to indicate that the features of the embodiment described may be combined with any other embodiment disclosed herein.

Claims

1. A method performed in a communication device (130) for handling network slices in a wireless communication network (100), the method comprising:

encrypting (610) Network Slice Selection Assistance information, NSSAI, using public key cryptography;

including (620) the encrypted NSSAI in a Non Access Stratum, NAS, registration request;

sending (630) a Radio Resource Control, RRC, connection request to a network node (111/112) including the NAS registration request.

2. The method according to claim 1, wherein the encryption is performed using Public Land Mobile Network, PLMN, public key.

3. The method according to any one of claims 1-2, further comprising:

including the encrypted NSSAI in the RRC connection request.

4. The method according to any one of claims 1-2, further comprising:

encrypting Network Slice Selection Assistance information, NSSAI, using Radio Access Network, RAN, public key;

including the encrypted NSSAI in the RRC connection request.

5. The method according to claim 4, wherein the RAN public key is specific for each network node or common for all network nodes in the RAN.

6. The method according to any one of claims 1-2, further comprising:

including an Access and Mobility Management Function, AMF, selection identifier in the RRC connection request.

7. The method according to claim 6, wherein the AMF selection identifier is pre-configured in the communication device or configured over a NAS in an initial registration.

8. A communication device (130) for handling network slices in a wireless communication network (100), the communication device (130) is configured to:

encrypt Network Slice Selection Assistance information, NSSAI, using public key cryptography;

include the encrypted NSSAI in a Non Access Stratum, NAS, registration request; and

send a Radio Resource Control, RRC, connection request to a network node including the NAS registration request.

9. The communication device (130) according to claim 8, wherein the encryption is performed using Public Land Mobile Network, PLMN, public key.

10. The communication device (130) according to any one of claims 8-9, is further configured to include the encrypted NSSAI in the RRC connection request.

11. The communication device (130) according to any one of claims 8-9, is further configured to:

encrypt Network Slice Selection Assistance information, NSSAI, using Radio Access Network, RAN, public key; and

include the encrypted NSSAI in the RRC connection request.

12. The communication device (130) according to claim 11, wherein the RAN public key is specific for each network node or common for all network nodes in the RAN.

13. The communication device (130) according to any one of claims 8-9, is further configured to include an AMF selection identifier in the RRC connection request.

14. The communication device (130) according to claim 13, wherein the AMF selection identifier is pre-configured in the communication device or configured over a NAS in an initial registration.

15. A method performed in a network node (111) for handling network slices for a communication device (130) in a wireless communication network (100), wherein the wireless communication network (100) comprises the network node (111) in a Radio Access Network, RAN, and a network function in a core network (140), CN, the method comprising:

receiving (710) a Radio Resource Control, RRC, connection request from the communication device; wherein the RRC connection request comprises a NAS registration request including a Network Slice Selection Assistance information, NSSAI, encrypted using Public Land Mobile Network, PLMN, public key;

selecting (720) a network function based on information in the RRC connection request;

forwarding (730) the NAS registration request to the network function;

forwarding (740) to the communication device a NAS registration response received from the network function after the network function decrypting the NSSAI using a PLMN private key.

16. The method according to claim 15, wherein *selecting* a network function is based on a Access and Mobility Management Function, AMF, selection identifier provided in the RRC connection request.

17. The method according to claim 15, wherein *selecting* a network function is based on a Radio Access Network, RAN, public key encrypted NSSAI provided in the RRC connection request.

18. The method according to claim 15, wherein *selecting* a network function is based on a default AMF if no AMF selection identifier is included in the RRC connection request.

19. The method according to claim 15, wherein *selecting* a network function is based on a PLMN public key encrypted NSSAI provided in the RRC connection request.

20. A network node (111) for handling network slices for a communication device (130) in a wireless communication network (100), wherein the wireless communication network (100) comprises the network node in a Radio Access Network, RAN, and a network function in a core network, CN, the network node (111) is configured to:

receive a Radio Resource Control, RRC, connection request from the communication device (130); wherein the RRC connection request comprises a NAS registration request including a Network Slice Selection Assistance information, NSSAI, encrypted using Public Land Mobile Network, PLMN, public key;

select a network function based on information in the RRC connection request;

forward the NAS registration request to the network function;

forward to the communication device a NAS registration response received from the network function after the network function decrypting the NSSAI using a PLMN private key.

21. The network node (111) according to claim 20, wherein the information in the RRC connection request is a Mobility Management Function, AMF, selection identifier.

22. The network node (111) according to claim 20, wherein the information in the RRC connection request is a Radio Access Network, RAN, public key encrypted NSSAI.

23. The network node (111) according to claim 20, wherein a network function is selected based on a default AMF if no AMF selection identifier is included in the RRC connection request.

24. The network node (111) according to claim 20, wherein the information in the RRC connection request is a PLMN public key encrypted NSSAI.

25. A method performed in a wireless communication network (100) for handling network slices for a communication device, wherein the wireless communication network (100) comprises a network node (111) in a Radio Access Network, RAN, and a network function in a core network (140), CN, of the wireless communication network (100), the method comprising:

receiving (810) in the network node (111) a Radio Resource Control, RRC, connection request from the communication device; wherein the RRC connection request comprises a NAS registration request including a Network Slice Selection Assistance information, NSSAI, encrypted using Public Land Mobile Network, PLMN, public key;

selecting (820) a network function in the network node (111) based on information provided in the RRC connection request;

forwarding (830) from the network node (111) to the network function the NAS registration request;

decrypting (840) in the network function the encrypted NSSAI using a PLMN private key;

receiving (850) in the network node (111) from the network function a NAS registration response;

sending (860) from the network node (111) to the communication device the NAS registration response.

26. The method according to claim 25, wherein *selecting* a network function is based on a Mobility Management Function, AMF, selection identifier provided in the RRC connection request.

27. The method according to claim 25, wherein *selecting* a network function is based on a Radio Access Network, RAN, public key encrypted NSSAI provided in the RRC connection request.

28. The method according to claim 25, wherein *selecting* a network function is based on a default AMF if no AMF selection identifier is included in the RRC connection request.

29. The method according to claim 25, wherein *selecting* a network function is based on a PLMN public key encrypted NSSAI provided in the RRC connection request.

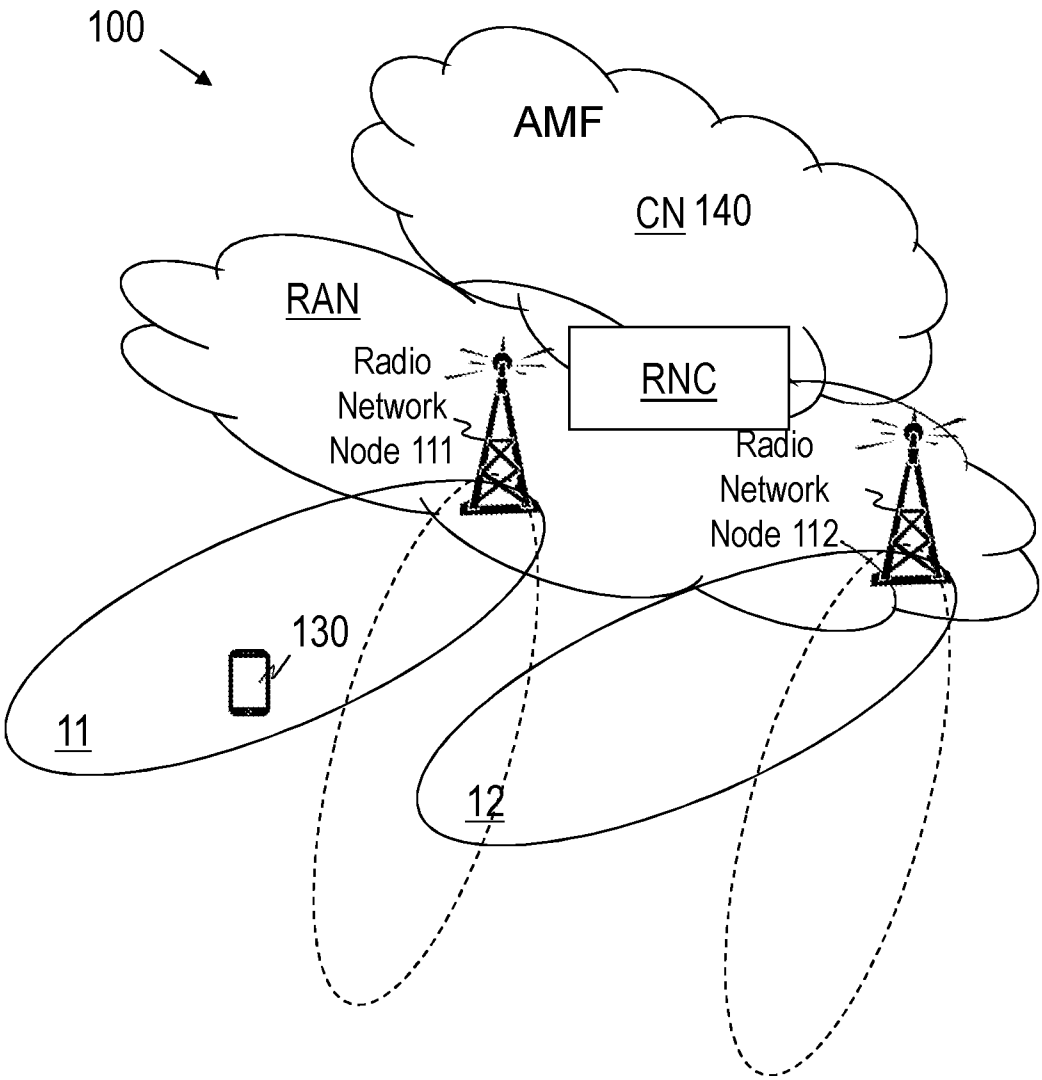
100
AMF
CN 140
RAN
Radio
Network
Node 111
RNC
Radio
Network
Node 112
130
11
12

Fig. 1

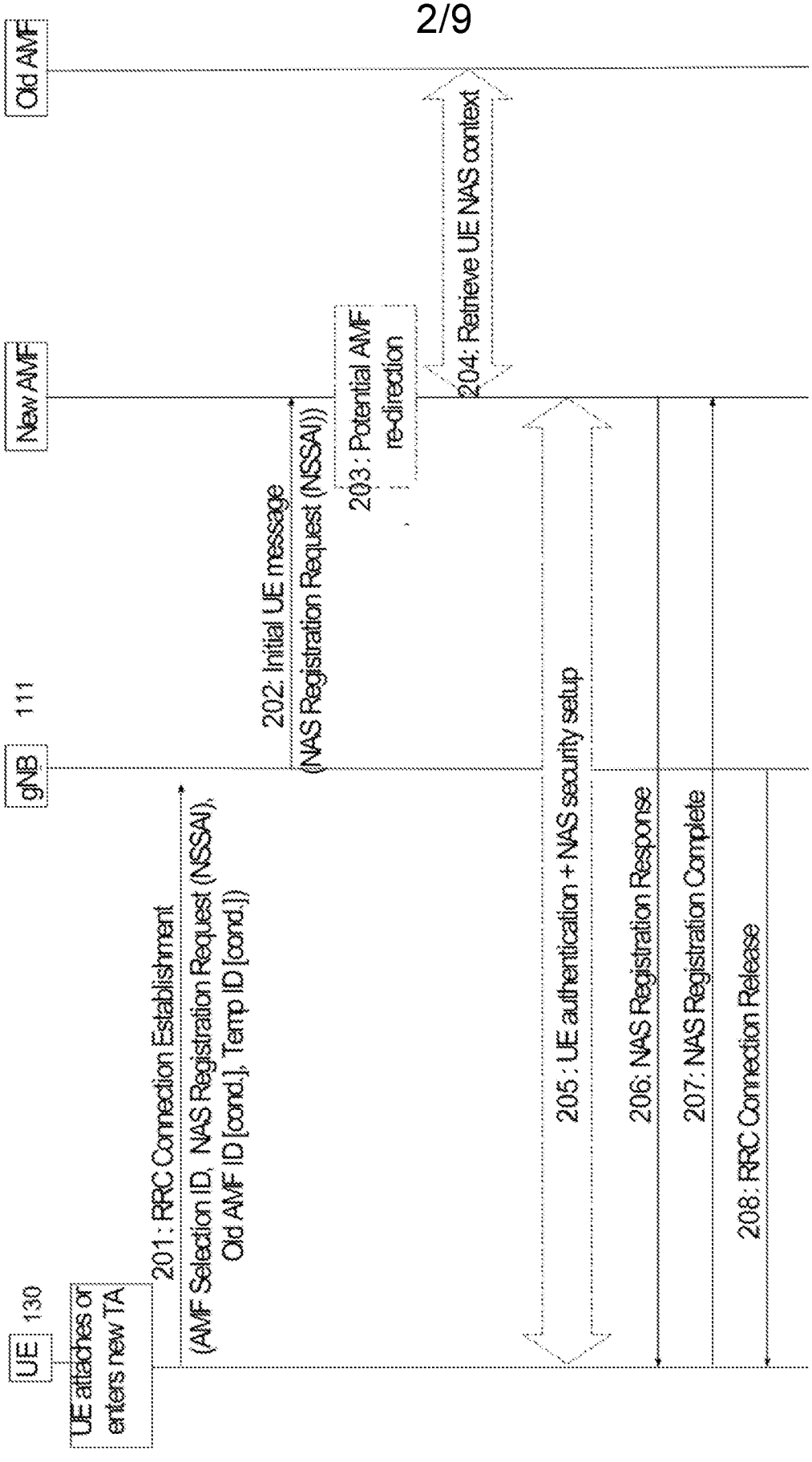
UE 130
gNB 111
New AMF
Old AMF
UE attaches or enters new TA
201: RRC Connection Establishment
(AMF Selection ID, NAS Registration Request (NSSAI), Old AMF ID [cond.], Temp ID [cond.])
202: Initial UE message
(NAS Registration Request (NSSAI))
203: Potential AMF re-direction
204: Retrieve UE NAS context
205: UE authentication + NAS security setup
206: NAS Registration Response
207: NAS Registration Complete
208: RRC Connection Release

Fig. 2

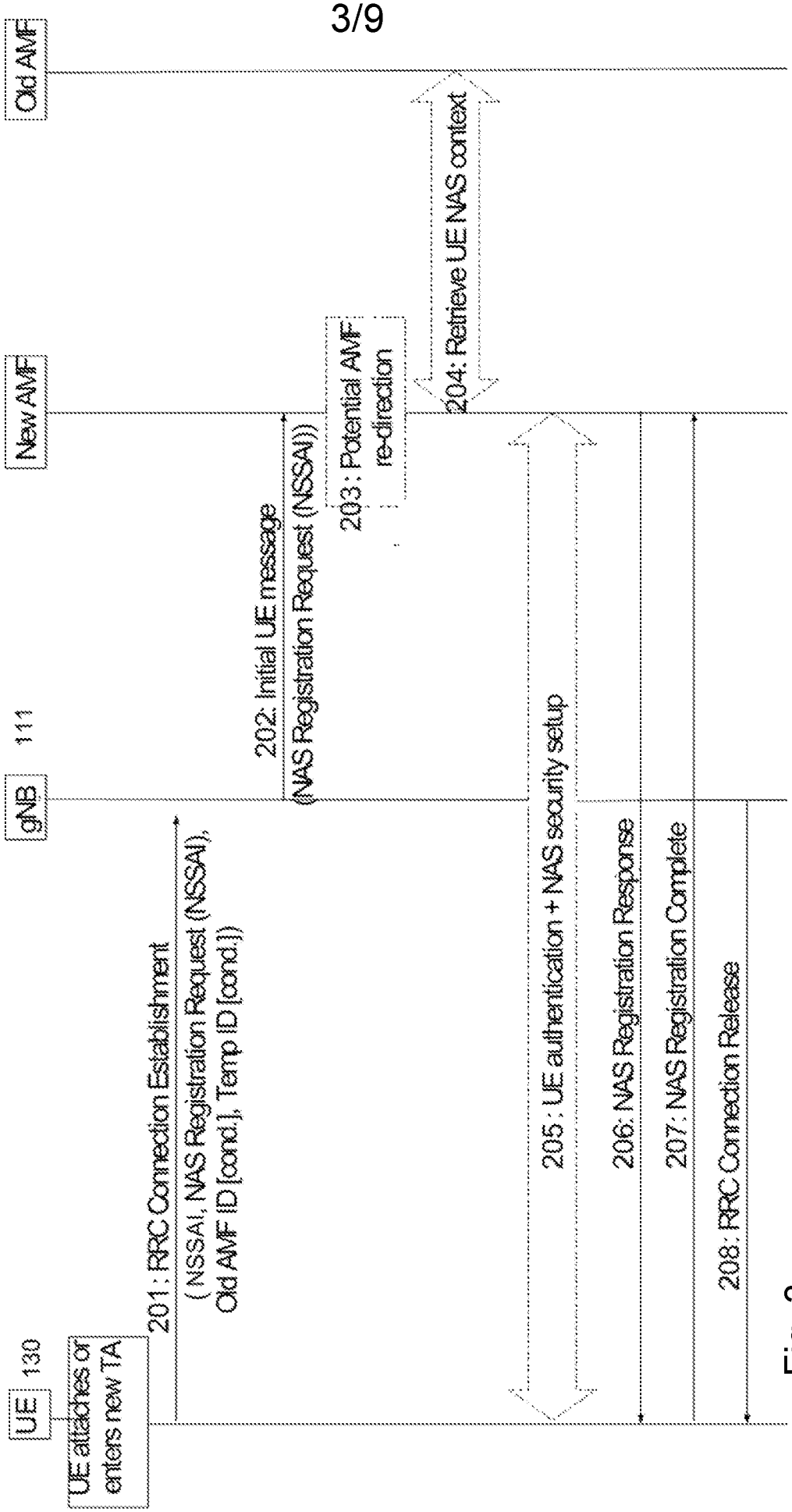
UE 130
gNB 111
New AMF
Old AMF
UE attaches or enters new TA
201: RRC Connection Establishment
(NSSAI, NAS Registration Request (NSSAI),
Old AMF ID [cond.], Temp ID [cond.])
202: Initial UE message
(NAS Registration Request (NSSAI))
203: Potential AMF re-direction
204: Retrieve UE NAS context
205: UE authentication + NAS security setup
206: NAS Registration Response
207: NAS Registration Complete
208: RRC Connection Release

Fig. 3

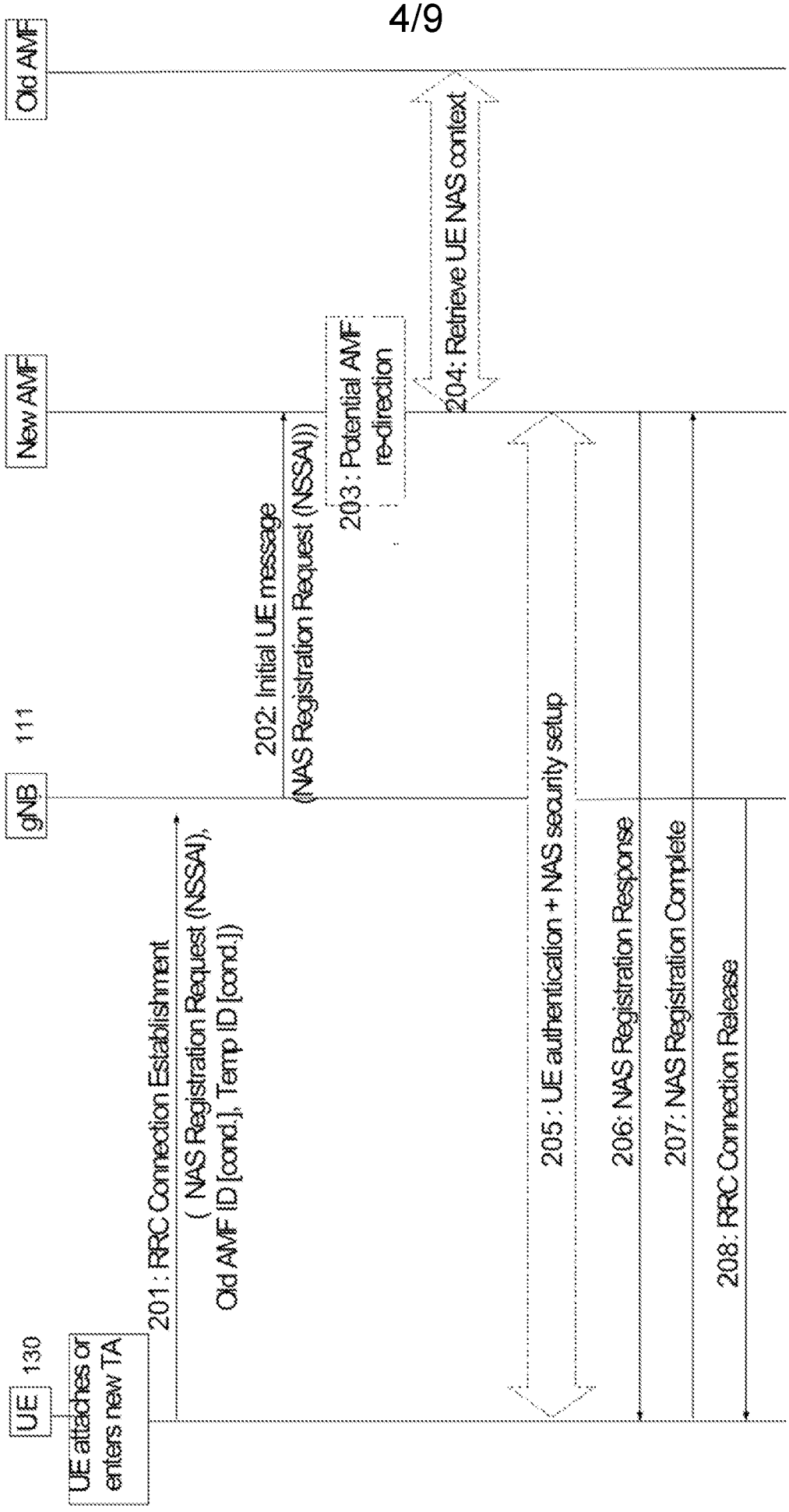
UE
130
gNB
111
New AMF
Old AMF
UE attaches or enters new TA
201 : RRC Connection Establishment
(NAS Registration Request (NSSAI),
Old AMF ID [cond.], Temp ID [cond.])
202: Initial UE message
(NAS Registration Request (NSSAI))
203 : Potential AMF re-direction
204: Retrieve UE NAS context
205 : UE authentication + NAS security setup
206: NAS Registration Response
207: NAS Registration Complete
208: RRC Connection Release

Fig. 4

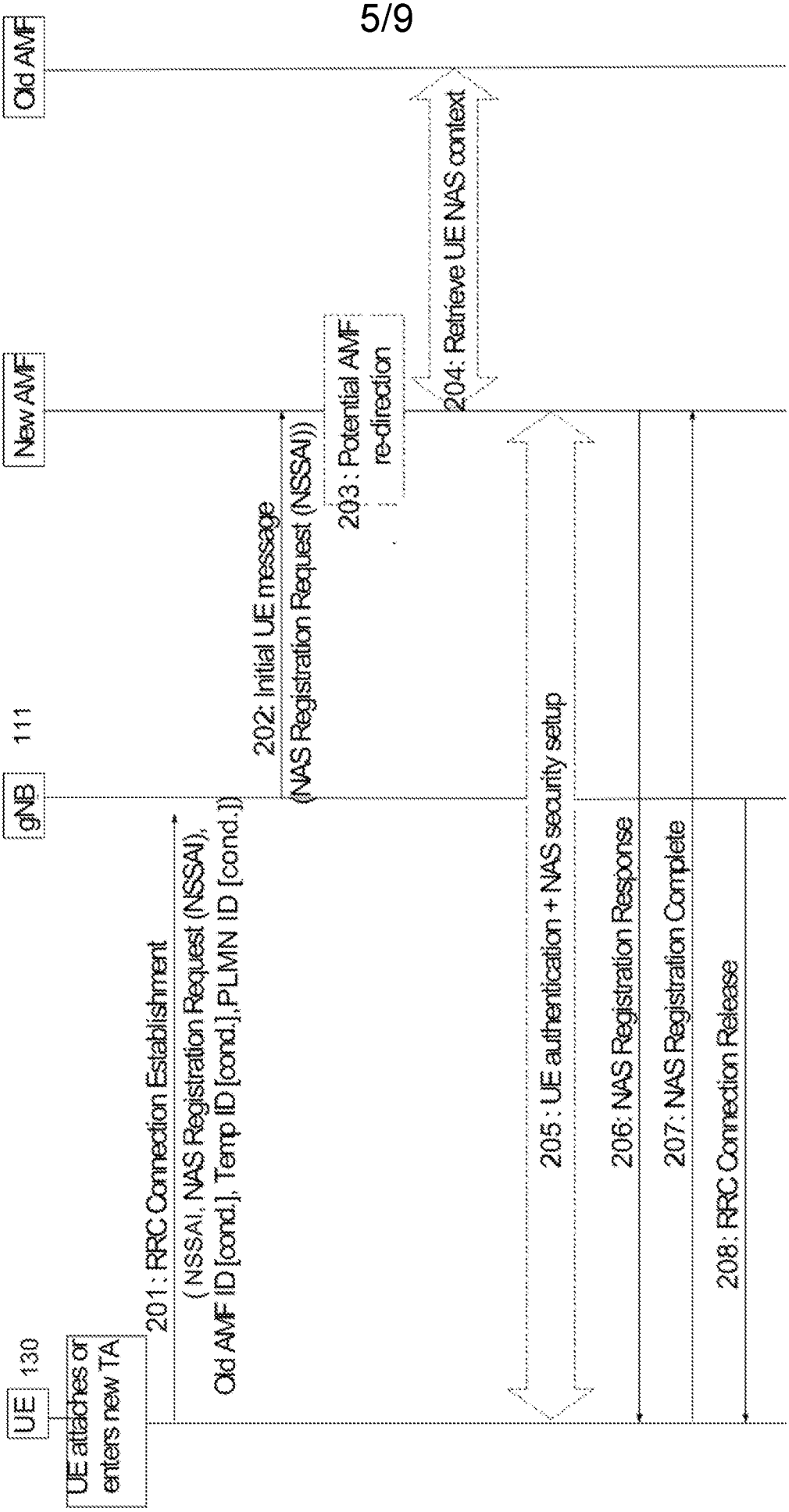
UE 130
gNB 111
New AMF
Old AMF
UE attaches or enters new TA
201: RRC Connection Establishment
(NSSAI, NAS Registration Request (NSSAI),
Old AMF ID [cond.], Temp ID [cond.],PLMN ID [cond.])
202: Initial UE message
(NAS Registration Request (NSSAI))
203: Potential AMF re-direction
204: Retrieve UE NAS context
205: UE authentication + NAS security setup
206: NAS Registration Response
207: NAS Registration Complete
208: RRC Connection Release

Fig. 5

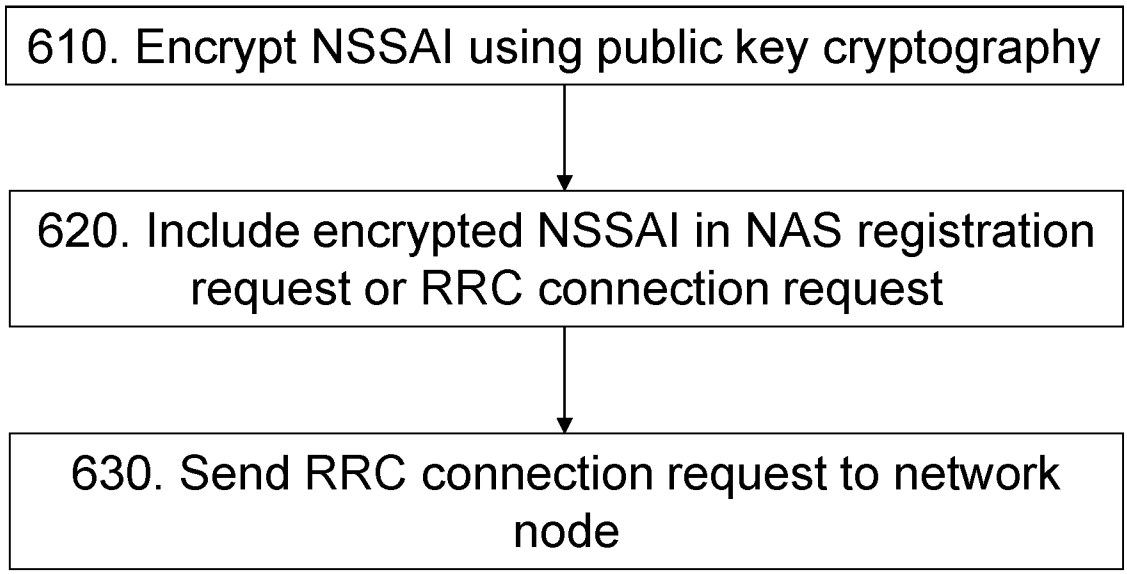
610. Encrypt NSSAI using public key cryptography
620. Include encrypted NSSAI in NAS registration request or RRC connection request
630. Send RRC connection request to network node

Fig. 6

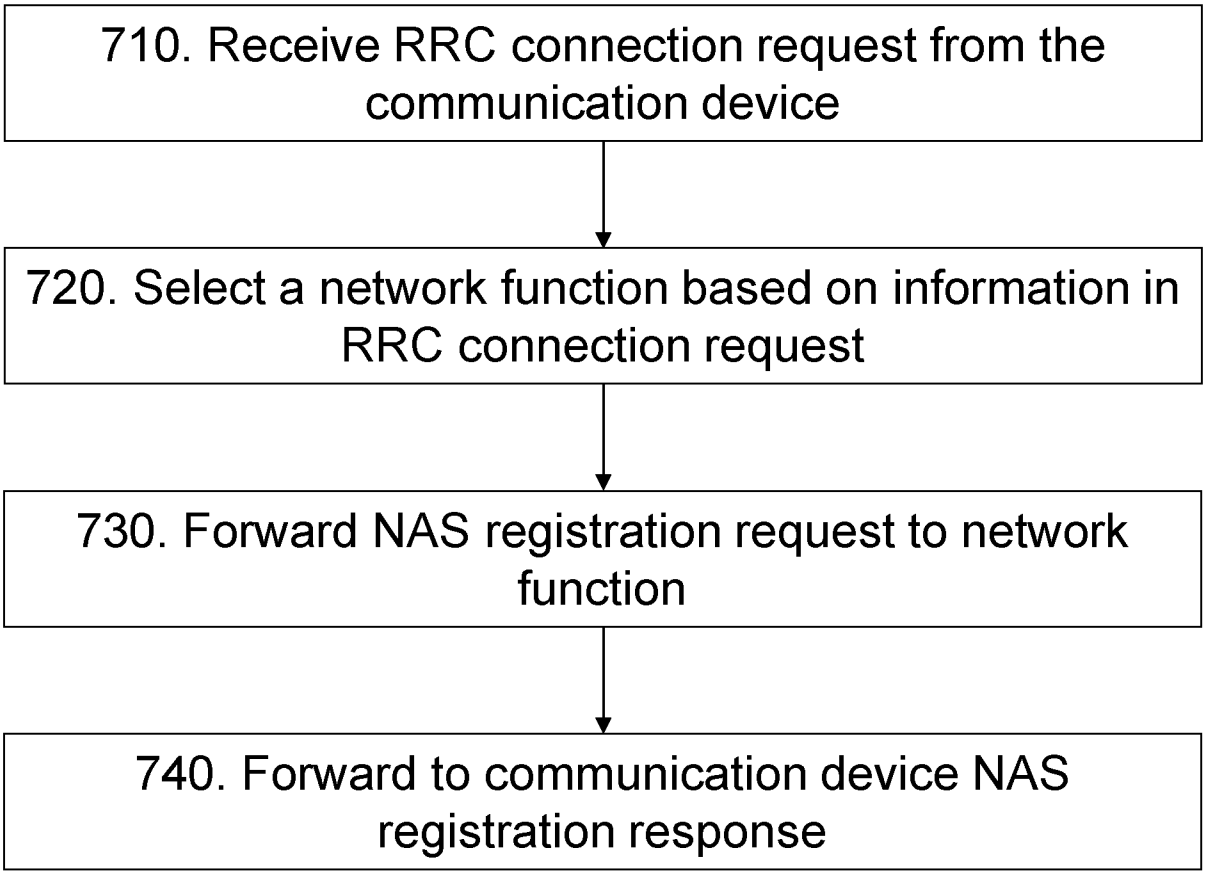
710. Receive RRC connection request from the communication device
720. Select a network function based on information in RRC connection request
730. Forward NAS registration request to network function
740. Forward to communication device NAS registration response

Fig. 7

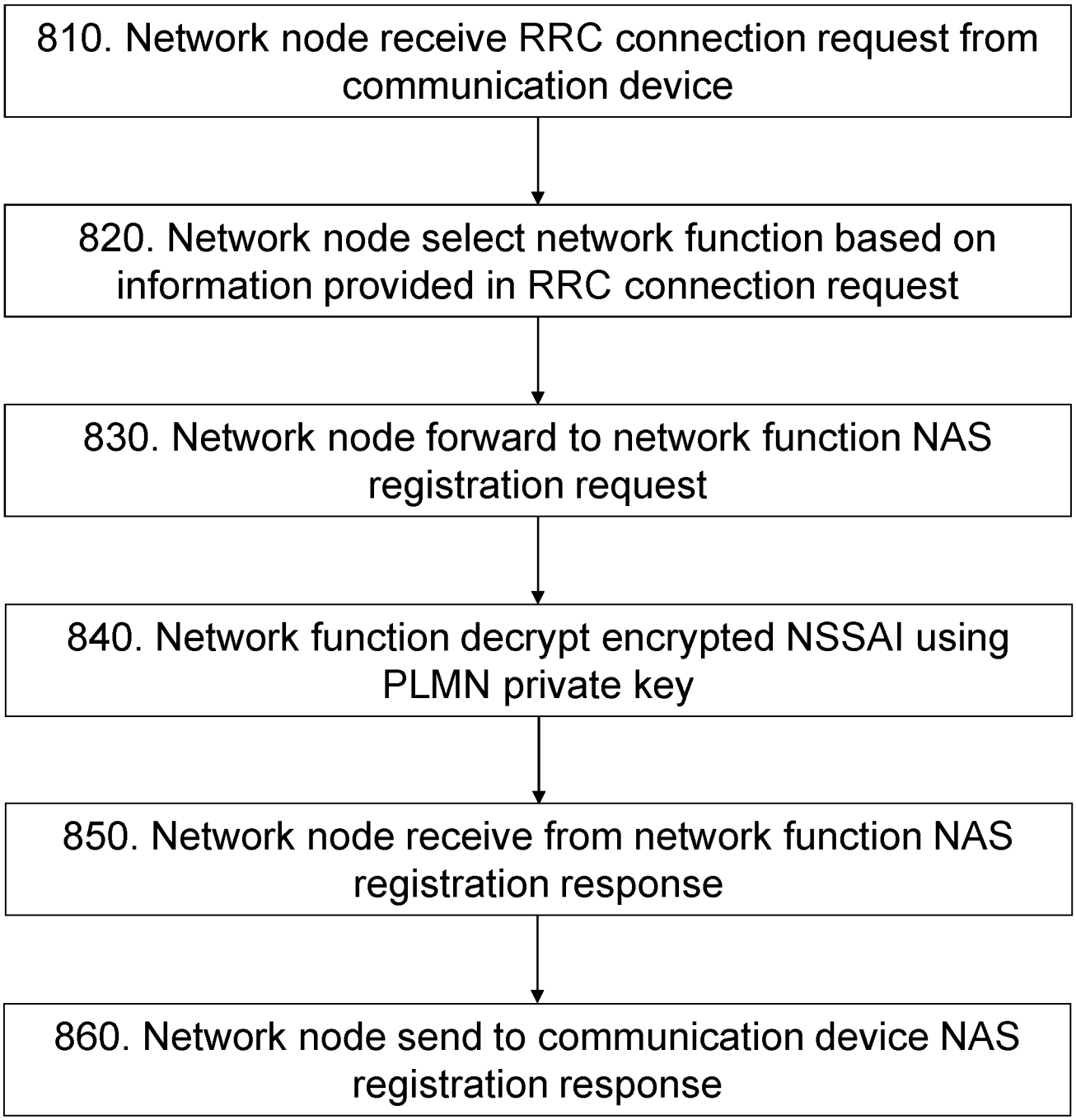
810. Network node receive RRC connection request from communication device
820. Network node select network function based on information provided in RRC connection request
830. Network node forward to network function NAS registration request
840. Network function decrypt encrypted NSSAI using PLMN private key
850. Network node receive from network function NAS registration response
860. Network node send to communication device NAS registration response

Fig. 8

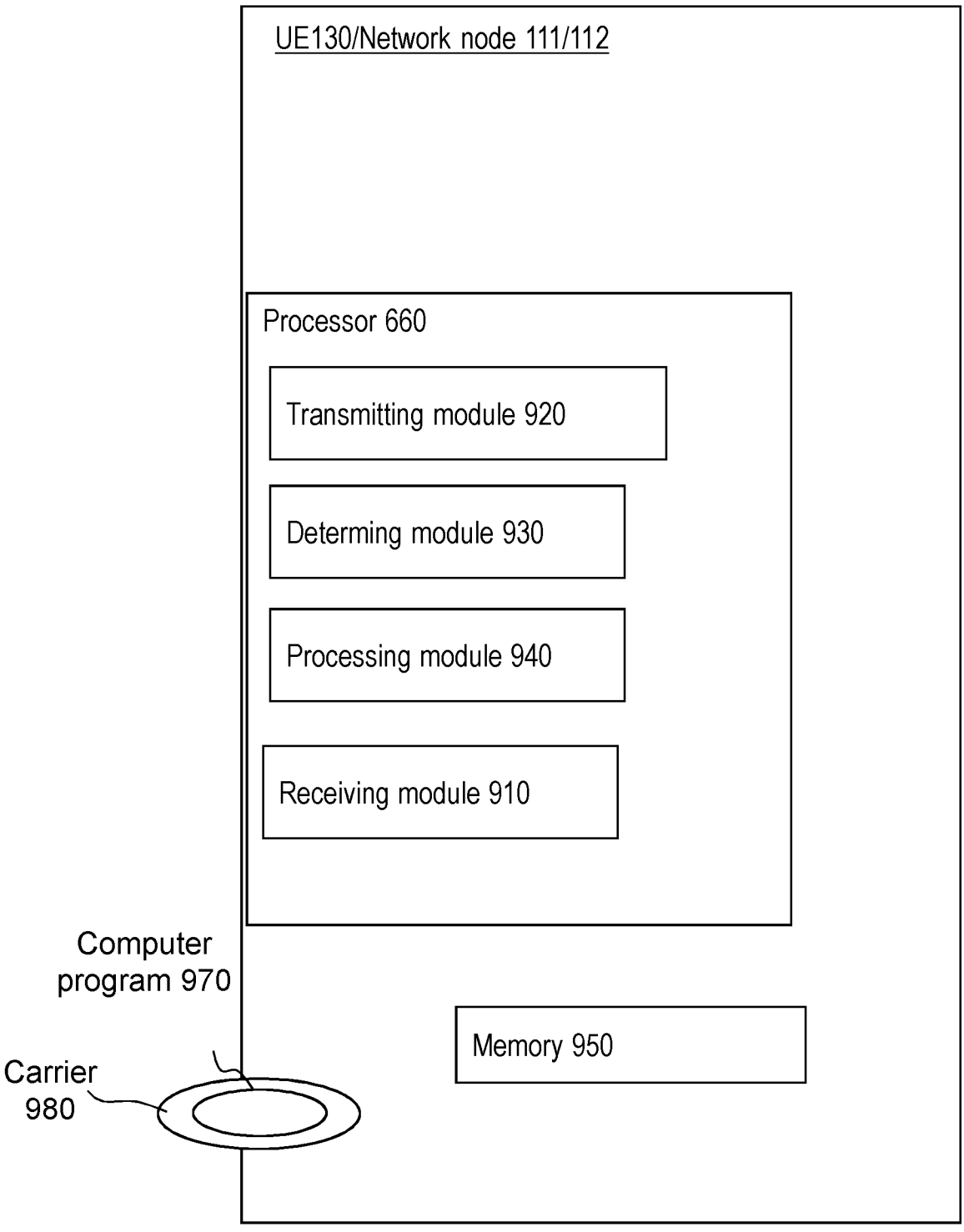
UE130/Network node 111/112
Processor 660
Transmitting module 920
Determing module 930
Processing module 940
Receiving module 910
Computer program 970
Memory 950
Carrier 980

Fig. 9

INTERNATIONAL SEARCH REPORT

International application No
PCT/SE2018/050576

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04W12/06 H04W48/18 H04W4/00 H04W12/02 H04L29/08
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04W H04L

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

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, INSPEC, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	HUAWEI: "Solution for Selection of Network Slice and CN entity", 3GPP DRAFT; R3-162460 CN ENTITY SELECTION, 3RD GENERATION PARTNERSHIP PROJECT (3GPP), MOBILE COMPETENCE CENTRE ; 650, ROUTE DES LUCIOLES ; F-06921 SOPHIA-ANTIPOLIS CEDEX ; FRANCE , vol. RAN WG3, no. Sophia Antipolis, France; 20161010 - 20161014 6 October 2016 (2016-10-06), XP051152108, Retrieved from the Internet: URL:http://www.3gpp.org/ftp/Meetings_3GPP_SYNC/RAN3/Docs/ [retrieved on 2016-10-06] page 2, lines 15-24; figure 2 page 3, line 1 - page 4, line 13; figures 9.2.x-1 ----- -/--	1-29

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
2 August 2018	13/08/2018

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Herzog, Till-Henning

INTERNATIONAL SEARCH REPORT

International application No
PCT/SE2018/050576

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2016/048574 A1 (QUALCOMM INC [US]) 31 March 2016 (2016-03-31) page 2, lines 15-24; figure 2 page 3, line 16 - page 4, line 13; figures 9.2.x-1	1-29
A	Constantinos F Grecas ET AL: "Introduction of the Asymmetric Cryptography in GSM, GPRS, UMTS, and Its Public Key Infrastructure Integration", Mobile Networks and Applications, 1 April 2003 (2003-04-01), pages 145-150, XP055496473, Boston DOI: 10.1023/A:1022285130956 Retrieved from the Internet: URL:https://link.springer.com/content/pdf/10.1023/A:1022285130956.pdf [retrieved on 2018-08-01] page 3, line 4 - page 5, line 37; figures 1,2,3	1-29
A	"3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Study on the security aspects of the next generation system (Release 14)", 3GPP DRAFT; S3-170962_TR33899-110_CL, 3RD GENERATION PARTNERSHIP PROJECT (3GPP), MOBILE COMPETENCE CENTRE ; 650, ROUTE DES LUCIOLES ; F-06921 SOPHIA-ANTIPOLIS CEDEX ; FRANCE , 13 April 2017 (2017-04-13), XP051269002, Retrieved from the Internet: URL:http://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_86b_Busan/Docs/ [retrieved on 2017-04-13] page 397, lines 28-30	1-29
X,P	WO 2017/200978 A1 (IDAC HOLDINGS INC [US]) 23 November 2017 (2017-11-23) paragraphs [0006], [0131], [0139], [0144], [0172] - [0207]; figures 16,17	1,2,8,9, 15,20,25

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/SE2018/050576

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2016048574 A1	31-03-2016	AU 2015321927 A1	16-03-2017
		BR 112017006156 A2	06-02-2018
		CN 106717044 A	24-05-2017
		CU 20170033 A7	04-07-2017
		EP 3198906 A1	02-08-2017
		JP 6235761 B2	22-11-2017
		JP 2017529799 A	05-10-2017
		KR 20170038096 A	05-04-2017
		PE 06562017 A1	17-05-2017
		TW 201626751 A	16-07-2016
		US 2016094988 A1	31-03-2016
		WO 2016048574 A1	31-03-2016
WO 2017200978 A1	23-11-2017	NONE	