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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
30 April 2015 (30.04.2015)

WIPO | PCT

(10) International Publication Number
WO 2015/059286 A1

(51) International Patent Classification:
H04L 29/06 (2006.01) *H04L 9/08* (2006.01)
H04W 12/04 (2009.01)

(21) International Application Number:
PCT/EP2014/072874

(22) International Filing Date:
24 October 2014 (24.10.2014)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
13190078.9 24 October 2013 (24.10.2013) EP

(71) Applicants: **KONINKLIJKE KPN N.V.** [NL/NL]; Maanplein 55, NL-2516 CK The Hague (NL). **NEDERLANDSE ORGANISATIE VOOR TOEGEPAST-NATUURWETENSCHAPPELIJK ONDERZOEK TNO** [NL/NL]; Schoemakerstraat 97, NL-2628 VK Delft (NL).

(72) Inventor: **DE KIEVIT, Sander**; Ravenhorst 61, NL-2317 AG Leiden (NL).

(74) Agent: **WUYTS, Koenraad**; P.O. Box 95321, NL-2509 CH The Hague (NL).

(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))*

(54) Title: CONTROLLED CREDENTIALS PROVISIONING BETWEEN USER DEVICES

(57) Abstract: The disclosure relates a method for controlling, by a first user device, user data exchange of a second user device over a telecommunications network. The first user device obtains a set of credentials and at least a portion of the set of credentials is provided to the second user device to enable the second user device to exchange user date over the telecommunications network. The data exchange of the second user device over the telecommunications network is controlled by the first user device. The first user device may perform a control action with respect to the credentials obtained by the first user device and provided to the second device.

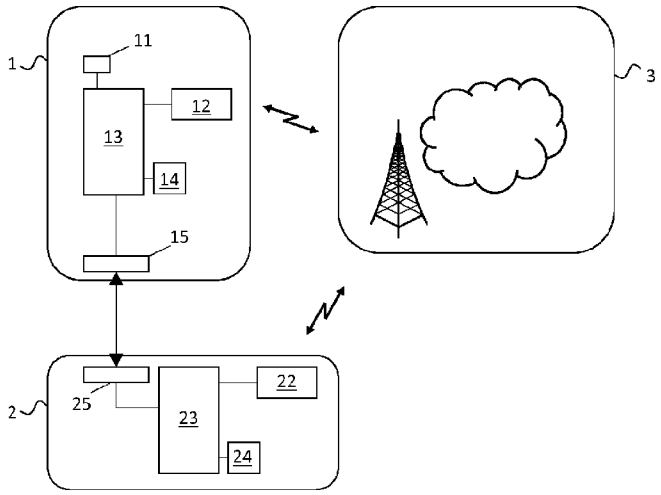

FIG. 1

WO 2015/059286 A1

Controlled credentials provisioning between user devices

FIELD OF THE INVENTION

The invention relates to controlled credentials provision between user devices. In particular, the invention relates to a control method by a first user device for user data exchange of a second user device over a telecommunications network, the control method enabling the first user device to stay in control when provisioning credentials from the first user device to the second user device.

BACKGROUND

Over the last years, the number of user devices, which can use or need connectivity has increased steadily. Currently, devices such as televisions, game consoles, camera's etc. come with facilities to connect to wifi access points or cabled in-house Ethernet. It is expected that in the upcoming years a typical household will have a hundred connected devices, a large part of which is portable (tablet, phone, game console, camera, navigation system, car keys, medical devices, watches, eyeglasses comprising cameras, electronic displays, etc.).

For some of these devices, connectivity is limited to wifi access points. Whereas that is not a problem for local devices, such as a refrigerator or heating system, for portable devices this means that when used on the move, access is only intermittent and often a burden to configure.

A solution to this problem would be to provide every user device with its own subscription in a telecommunications network comprising a wireless access network. Although such a solution would provide access while traveling, it comes with a burden of managing all the different subscriptions (potentially with different providers) for all the different devices for both the user and the operator of the telecommunications network. Moreover, every subscription may likely come with its own subscription fee. Therefore an easier solution is necessary that provides the user with sufficient flexibility to provide connectivity for devices while on the move. These devices comprise any of the devices mentioned in the previous paragraph and can be portable or integrated in a vehicle, in a machine or in an apparatus, e.g. household appliances.

US 2012/0129498 discloses a method and device for allowing a wireless communication device initially unauthorized for communication with a network to obtain persistent soft network subscription credential information from a wireless communication device initially authorized for communication with the network. The transfer of the subscription credentials from one device to another authorizes the previously unauthorized device to become authorized for communication with the network. The method ensures that only one communication device is capable of communicating with a network at any one time.

The prior art method and device allows user data exchange over the telecommunications network for multiple user devices by obtaining credential information from another device. Only the latter device needs to have a subscription with the telecommunications network. However, the prior art method assumes complete trust of the (user of the) devices obtaining the credential information from the device originally having the credential information.

SUMMARY

The present disclosure presents a method wherein a device, referred to as second user device or slave device, may be provided with credential information obtained by another user device, referred to as first device or master device. The first user device maintains some form of control over the user data exchange of the second user device over the telecommunications network while having provided credentials to the second user device. This form of control may e.g. include a control action from the first user device to abort the user data exchange of the second user device over the telecommunications network.

In one aspect of the disclosure, a method for controlling, by a first user device, user data exchange of a second user device over a telecommunications network. Both the first user device and the second user device are configured to wirelessly connect to the telecommunications network (i.e. both devices have wireless access capabilities, but the second user device may not be authorized to access the telecommunications network, e.g. because it has no subscription and therefore does not have or cannot obtain credentials on its own).

The first user device obtains a set of credentials, e.g. over the telecommunications network or from a (U)SIM or by deriving credentials from information received over the telecommunications network and/or from the (U)SIM. The credentials comprise information enabling wireless access to and secure communication over the telecommunications network and include an identifier (e.g. a temporary identifier, such as a T-IMSI) and a plurality of keys (both for user data transmission and for signalling data transmission) for signal transmission over the network.

At least a portion of, but possibly the complete, set of credentials is provided to the second user device to enable the second user device (which did not yet have the credentials required for authorized access to the network, for example because it did not have a separate subscription) to exchange user data over the telecommunications network.

The data exchange of the second user device over the telecommunications network is controlled by the first user device. To that end, the first user device performs a control action with respect to the credentials obtained by the first user device and provided to the second device. Various options for such control are disclosed in the embodiments described below.

Another aspect of the disclosure relates to a computer program comprising software code portions configured for, when executed on a computer system, performing the method disclosed herein.

A still further aspect of the disclosure relates to a non-transitory computer program medium comprising the computer program.

Still further, a user device configured with the computer program is disclosed.

In all of these aspects, the first user device is given control of the data exchange of the second user device by means of a control action related to a set of credentials obtained by the first user device while not requiring a separate subscription for the second user device. This enables the first user device to provide credentials to the second user device without assuming a complete trust. If for any reason, the first user device desires to abort the user data exchange of the second user device, it can perform the control action.

It should be appreciated that the first user device and the second user device are separate devices. For example, the first user device and second user device each have a baseband processor and software such that both are configured to wirelessly connect to the telecommunications network.

It should further be appreciated that the credentials (identifier, signal transmission key(s)) may also be derived by the first device from information received by the first user device.

In one embodiment, the first user device obtains a set of credentials and provides the complete set of credentials to the second user device. The set of credentials would allow the first user device, if the first user device would apply the credentials itself, to exchange user data over the telecommunications network. An advantage of providing a complete set of credentials to the second user device is that handovers within a telecommunications network and between telecommunications networks with different radio access technologies (RATs) are possible for the second user device without the intervention of the first user device.

In this case, the control action of the first user device may comprise instructing the telecommunications network to invalidate the identifier and/or the keys provided to the second user device. Either of these control actions would at some point in time disable user data exchange for the second user device.

In another embodiment, the first user device obtains a set of credentials but only provides a portion of the set of credentials to the second user device. An advantage of this embodiment is that increased control options are available for controlling the user data exchange of the second user device over the telecommunications network. Examples include modifying one or more credentials retained in the first user device and/or invalidating one or more of the credentials provided to the second user device.

In one embodiment, the signal transmission keys of the set of credentials are organized in a key hierarchy, wherein a key lower in the key hierarchy is derived from a key higher in the key hierarchy. Such a key hierarchy exists e.g. for the 4G LTE telecommunications network or for a next generation telecommunications network. The portion of the keys provided to the second user device may e.g. consist of one or more signal transmission keys lower in the key hierarchy. The keys retained in the first user device, i.e. not provided to the second device, may e.g. consist of keys higher in the key hierarchy. The control action by the first user device may comprise generating new higher keys, thereby making the lower keys (derived from the higher keys) invalid. This control action by the first user may be performed without any cooperation of the second user device (and can therefore also not be blocked by the second user device) for the key generation and derivation is performed by the first user device and the telecommunications network.

In another embodiment, the only signal transmission key provided to the second user device is a user plane encryption key used to encrypt user data over the radio part of the network. The first user device provides further user data inclusion details to the second user device, e.g. by a direct connection to the baseband processor of the second user device. In this manner, the first user device provides user data inclusion details, i.e. informs the second user device where to insert and/or retrieve user data in

the user data transmission to/from the first user device. The first user device can control any credential remaining in the first user device to control the user data exchange via the second user device.

In yet another embodiment, control may be performed by the first user device by maintaining at least part of the signaling information transmission for the user data exchange of the second user device with the first user device. Accordingly, manipulating the signaling information or the transmission thereof enables control by the first user device of the user data exchange of the second user device.

In one particular example thereof, the telecommunications network comprises an LTE network and the set of credentials obtained by the first user device includes one or more non-access stratum (NAS) keys. The NAS keys are kept with the first user device and the control action from the first user device in relation to the NAS key may comprise transmitting a NAS message Detach Request to the telecommunications network (in particular to the MME and/or transmitting an authentication failure message upon receiving a challenge from the telecommunications network during a Tracking Area Update (TAU). The advantage of this embodiment is that the control actions comply with procedures currently provided in the 3GPP standards 3GPP TS 23.401 and 3GPP TS 33.102, respectively.

Another particular example involves a next generation network wherein user data transmission and signalling transmission will even be further separated than for LTE networks. For next generation networks, the physical connections for user data transmission and for signalling may be different for the first user device and the second user device, enabling the first user device to control a physical data connection of the second user device by controlling the physical signalling connection on the first user device.

In one embodiment of the disclosure, the method comprises applying a first identifier from the telecommunications network enabling the first user device to exchange user data over the telecommunications network and requesting a second identifier from the telecommunications network. The second identifier may be provided to the second user device to enable the second user device to exchange user data over the telecommunications network. In this manner the telecommunications network may be informed of the transfer of the credentials to the second user device. An advantage of this method is that both the first user device (via the first identifier) and the second user device (via the second user identifier) may connect to the telecommunications network for the exchange of user data.

In another embodiment, the first user device provides its own user identifier to the second user device. In this manner the network does not need to support the existence of two user devices with two respective identifiers under one subscription.

In yet another disclosed embodiment, the method comprises the step of establishing a direct connection, such as an LTE direct connection or a Bluetooth connection, between the first user device and the second user device for at least providing the at least portion of the set of credentials to the second user device. This step is particularly useful for embodiments wherein only a portion of the set of credentials is provided to the second user device.

In one embodiment, the first user device obtains one or more sets of credentials in advance and provides one or more of the sets of credentials to one or more second user devices at a later

time. In this manner, the first user device does not need to establish his own connection with the telecommunications network before providing the one or more credentials to the second user device.

In one embodiment, the first user device provides its identifier to the second user device. The second user device connects to the telecommunications network using the identifier and receives information from the telecommunications network. The information is forwarded to the first user device to derive one or more credentials, such as one or more signal transmission keys. An example of such a process is a challenge-response process with the telecommunications network. The first user device provides one or more of the derived credentials to the second user device.

It should be appreciated that the control action by the first user device may contain time information informing the network when the user data exchange should no longer be allowed. The time information would comprise a validity time for the credentials provided to the second user device. This information may be provided to the network at any suitable time prior to the moment that the data connection for the second user device should be disabled or not allowed anymore.

It is noted that the invention relates to all possible combinations of features recited in the claims.

BRIEF DESCRIPTION OF THE DRAWINGS

Aspects of the invention will be explained in greater detail by reference to exemplary embodiments shown in the drawings, in which:

FIG. 1 is a schematic illustration of system comprising a first user device and a second user device in combination with a telecommunications network;

FIG. 2 is a time diagram illustrating an embodiment of the disclosed method;

FIG. 3 is a general overview diagram of an LTE network and a 3G network;

FIG. 4 is an illustration of the key hierarchy in the LTE network shown in FIG. 3;

FIGS. 5-8B are various embodiments of methods wherein the first user devices provides a portion of the credentials to the second user device;

FIG. 9 is an embodiment of a method wherein the first user device only provides a user plane key to the second user device;

FIGS. 10-12 are various embodiments of methods wherein the first user device provides all of the user credentials to the second user device; and

FIGS. 13 and 14 provide an embodiment for a next generation network.

DETAILED DESCRIPTION OF THE DRAWINGS

FIG. 1 is a schematic illustration of a system comprising a first user device 1 and a second user device 2 in combination with a telecommunications network 3.

First user device 1 comprises a USIM 11 authorizing the first user device 1 to wirelessly access the telecommunications network 3 using baseband processor 12. First user device 1 further comprises a general processor 13 and a storage 14.

Second user device 2 comprises a baseband processor 22, a general processor 23 and a storage 24. The second user device may not contain a USIM.

First user device 1 comprises a direct communication interface 15 and second user device 2 comprises a direct communication interface 25 over which a direct connection can be established. The direct connection is a one-to-one connection independent from the telecommunications network 3. Examples include LTE direct, Bluetooth, infrared etc.. Processors 13, 23 may run a discovery protocol detecting the presence of other devices capable of establishing such a direct connection.

By virtue of the information in the USIM 11, the first user device is a device that may on its own access the telecommunications network 3 and exchange user data over the telecommunications network 3. The USIM 11 typically contains subscription information, such as an IMSI and a master key enabling the telecommunications network 3 to recognize the first user device 1 as a device with a subscription to subsequently provide the first user device 1 with the necessary information, such as keys or information from which key(s) can be derived. Examples of such devices include cellular telephones, tablet computer, laptops etc.

The second user device 2 does not contain a USIM (or cannot or does not want to use the USIM). However, similarly to the first user device 1, the second user device 2 is equipped with a baseband processor 22 that would, when it would have access to credentials, enable the second user device 2 to access the telecommunications network 3. It is expected that in the upcoming years, devices such as the second device 2 will find their way into households. Such devices may include devices presently enabled to access wifi access points, such as tablets, phones, game consoles, camera's, navigations systems, car keys, medical devices, watches, eyeglasses comprising cameras, electronic displays, etc. The second user device 2 preferably also is a portable device. The second device 2 may also comprise a machine or a household appliance.

FIG. 2 is a time diagram illustrating an embodiment of provisioning the second user device 2 with credentials to enable access and data exchange over the telecommunications network 3 for the second user device 2 without originally possessing such credentials. The credentials comprise or consist of one or more (temporary) identifiers under which a device is known in the network and one or more keys or derived keys.

In step S1, first user device 1 contacts the telecommunications network 3 in a manner known as such using some information stored in the USIM 11 and obtains information from the network 3 in step S2. The information may e.g. contain a temporary identifier (T-IMSI) and information from which, in combination with the master key stored in USIM 11, one or more keys may be derived, step S3. The T-IMSI and the derived keys constitute the credentials that the first user device 1 may use to access the telecommunication network 3 for exchanging data over the telecommunications network 3. The credentials may be stored in memory 14.

Then, in step S4, the first user device 1 provides some or all of the credentials to the second user device 2. Preferably, these credentials are transferred from the first user device 1 to the second user device 2 over the direct connection established between direct communication interfaces 15,25. The second user device may store the received credentials in memory 24.

Then, in step S5, the second user device 2 accesses the network 3 using baseband processor 22 and the credentials stored in memory 24 as obtained from the first user device 1.

In step S6, the second user device 2 is now enabled to exchange user data over the telecommunications network 3.

In one disclosed aspect, however, the first user device 1 stays in control over the data exchange of the second user device 2. In particular, this control is independent of the second user device 2, such that the second user device 2 cannot frustrate the control. This control, performed either solely by the first user device or by cooperation of the first user device 1 and the network 3, is illustrated schematically by the dashed lines around step S6. The control may be time-dependent, i.e. the first user device may inform the network that the data exchange of the second user device 2 should no longer be possible or continued after a particular moment in time derived from the time information.

The control scope by the first user device 1 depends on the credentials provided to the second user device. For example, the first user device 1 may inform the network 3 that the temporary identifier T-IMSI provided to the second user device 2 should no longer be considered a valid identifier. Another example may be to initiate a key refresh procedure for a key under control of the first user device 1 such that another key provided to the second user device 2 that is derived from the key under control of the first user device 1 becomes invalid.

Before providing various more detailed examples with reference to FIGS. 5-12, a brief description of a Long Term Evolution (LTE) network 3 will be provided with reference to FIG. 3 and of the various keys used in such a network with reference to FIG. 4.

FIG. 3 is a schematic illustration of a telecommunications network 3.

The upper branch in FIG. 3 represents a next generation network, commonly indicated as Long Term Evolution (LTE) or Evolved Packet System (EPS). Such a network comprises a PDN Gateway (P-GW) and a Serving Gateway (S-GW). The E-UTRAN of the EPS comprises evolved NodeBs (eNodeBs or eNBs) providing wireless access for a device 2 that is connected to the S-GW via a packet network. The S-GW is connected to a Home Subscriber Server HSS and a Mobility Management Entity MME for signalling purposes. The HSS may include a subscription profile repository SPR containing subscription information of user device 1.

Further information of the general architecture of a EPS network can be found in 3GPP TS 23.401.

The lower branch of FIG. 3 represents a GPRS or UMTS network comprising a Gateway GPRS Support Node (GGSN), a Serving GPRS Support Node (SGSN) and a Radio Access Network (RAN or UTRAN). For a GSM/EDGE radio access network (GERAN), the RAN comprises a Base Station Controller (BSC) connected to a plurality of Base (Transceiver) Stations (BSs, BTSs), both not shown. For a UMTS radio access network (UTRAN), the RAN comprises a Radio Network Controller (RNC) connected to a plurality of NodeBs), also not shown. The GGSN and the SGSN are conventionally connected to a Home Location Register (HLR) or Home Subscriber Server (HSS) that may contain subscription information of the user devices 1.

The telecommunications network 3 enables establishing connections for user data, also referred to as data sessions or as PDP Contexts, between a server system 40 and a user device 1 over a packet data network 41, wherein access of the user device 1 to the telecommunications network 3 is wireless.

Fig. 4 is a schematic illustration of a key hierarchy for an LTE telecommunications network.

A key, K_{ASME}, is generated in both the first user device and the network (more specifically, the authentication centre AuC) from integrity key IK, cipher key CK and a serving network id in a known manner. From the generated key K_{ASME}, keys for the protection of NAS signalling, RRC signalling and user plane communication on the radio interface are generated, as illustrated in Fig. 4.

The NAS keys K_{NASenc} en K_{NASint} used for encryption of session management between the first user device and the MME. Keys K_{UPenc}, K_{RRCInt}, en K_{RRCenc} are used at the radio interface between the UE and the base station eNodeB. These keys are derived using an intermediate key K_{eNB}. The K_{RRC} keys are access stratum keys used for the radio resources signalling. User plane key K_{UP} is used for encryption of the (user plane) traffic on the radio interface.

Control of the data exchange of the second user device may be based on any of the keys obtained by the first user device. For example, if the user plane key K_{UP} has been provided to the second user device, control can be exercised by the first user device through initiating a key refresh for either one of the NAS or RRC keys. Similarly, if the RRC keys or the NAS keys have been provided to the second user device, control can be performed on the basis of the user plane and/or NAS keys or on the basis of the user plane and/or RRC keys, respectively. If key K_{ASME} is provided to the second user device, the first user device may perform control by requesting the network to initiate a new AKA.

Similar control options exist for other types of networks, including the UTMS and GPRS networks as discussed briefly with reference to Fig. 3.

Some embodiments for the LTE network will now be described in further detail with reference to Figs. 5-12.

In Fig. 5, it is assumed that the first user device 1 and second user device 2 have been paired at some time t_0 and have setup a direct connection. A session may be going on between the first user device 1 and the network. At some later time $t_1 = t_0 + dt$, the first user device 1 would like to go into battery saving mode or forward an ongoing call to the nearby second user device 2. In step i), the first user device 1 informs the network that it would like to transfer the call / session to the second user device. In step ii), the network provides the first user device 1 with a temporary identifier X and a key or key identifier (an identifier signaling which key to use or which information to use to derive a key) to be used by the second user device 2. In step iii), the first user device 1 provides the second user device 2 with just the identifier X over the direct link and the identifier of the network it can reach. In step iv), the second user device 2 then connects to the network using the identifier X.

In step v), the network initiates an AKA (with a challenge). This could be any standardized LTE AKA. The second user device 2 forwards the challenge to the first user device 1 in step vi). In step vii), the first user device 1 calculates the response and sends it to the second user device 2 which

forwards it to the network. The network compares the response to the expected response and provides an OK to the second user device 2 which forwards it to the first user device 1 in step viii).

In step ix), the first user device 1 provides a set of keys to the second user device 2. These keys may e.g. contain the user plane key K_{UP} and the radio resource key K_{RRC}. With these two keys, the second user device 2 can decrypt and insert the user plane traffic and behave properly on the radio channel as long as it remains in reach of one eNodeB in the E-UTRAN. For hand-overs, etc. (which require a key on a higher level) the second user device 2 consults the first user device 1 for all the procedures. For session management, which require non-access stratus keys K_{NAS}, the second user device 2 also relies on the first user device 1. In this manner, the first user device remains in control of the connection and can quickly disable the second user device if necessary or desired.

Optionally, in case a user data session (e.g. call, video stream) was open between the first user device 1 and the network at this moment, the first user device 1 or an entity within the network may initiate a hand-over from the first user device 1 to the second user device 2 as shown in step x). At the network side, this requires that the session is rerouted to the second user device 2 (i.e. changing the address of the destination traffic) and encrypted with the new keys. At the first user device 1, application specific information is forwarded to the second user device 2 as shown in step xi). This means that the second user device 2 is informed about what application traffic is to be expected (e.g. VoIP traffic, video stream, Facebook traffic) and what traffic should be handled in the second user device 2 (e.g. VoIP and video) and what should be forwarded to the first user device 1 (e.g. Facebook and email retrieval). Such a mechanism is easily implemented on the TCP/IP layer, where the destination port numbers correspond to certain applications. The second user device 2 can then selectively forward traffic. The second user device 2 may forward at least the NAS signaling to the first user device 1 (the second user device 2 itself has no NAS keys) likely some application traffic is forwarded as well. The connection can be terminated by initiating a key refresh procedure, thereby invalidating the keys of the second user device 2.

It is noted that in the embodiment of Fig. 5, even before the first user device 1 and the second user device 2 have established a direct connection, the first user device 1 could already have requested and performed an AKA and store this information. The first user device 1 may now inform a second user device 2 to become a slave device on its behalf. In this manner, fewer steps may be necessary to set up the connection.

The keys provided to the second user device 2 do not enable a handover for the second user device 2 to a network with a different radio access technology (inter-RAT handover). If the second user device 2 has keys for an LTE network, these keys cannot be used for a UMTS network or for a GSM network. However, such handovers may still be performed within the mechanism as presented in this disclosure.

In a first solution, the second user device 2 may obtain all credentials from the first user device 1 necessary for a full UMTS or GSM connection. The second user device 2 detects that LTE coverage is ending and that UMTS or GSM are available in a manner known as such. The second user device 2 initiates an attach to the UMTS/GSM network. The network then initiates an AKA, which the second user device 2 forwards to the first user device 1. The first user device 1 and the network derive

new keys to be used in the UMTS (two keys) or GSM (one key) case. The direct connection between the first user device 1 and the second user device 2 may or may not remain. The first user device 1 may no longer have a signaling path to the network in this case. However, the first user device 1 itself may still be allowed to connect to the LTE network (if possible) and the session signaling could then be protected using the same keys that were used before. In order to have both the first user device 1 and the second user device 2 connected to different networks in this manner, extra signaling between the core network components of the LTE network (to which the first user device 1 is connected) and the UMTS network (to which the second user device 2 may be connected) may be arranged for.

In a second solution, if a handover is required, the direction of the traffic between the first user device 1 and the second user device 2 may be reversed. The direct connection between the first user device 1 and the second user device 2 is kept and the first user device 1 connects to the UMTS or GSM network. The first user device 1 receives the user data from the second user device 2 and forwards the user data to the network. An advantage of this second solution is that even if the handover cannot be performed by second user device 2, the exchange of user data of second user device 2 can continue via first user device 1.

In the embodiment of Fig. 6, the network is not informed about the transfer of a part of the credentials from the first user device 1 to the second user device 2. The advantage of the embodiment of Fig. 6 is that no network support is required for a connection of the second user device with the network.

The first user device 1 and second user device 2 are paired at some time t_0 and have established a direct connection. At some later time $t_1 = t_0 + dt$, the first user device 1 would like to go into battery saving mode or let the second user device 2 handle incoming traffic on its behalf. This can be done if no session is currently active.

In comparison with the embodiment of Fig. 5, the network does not need to be informed such that steps i) and ii) of Fig. 5 wherein the network was informed can be omitted.

In step iii), the first user device 1 provides the second user device 2 with its own identifier Y over the direct link and the identifier of the network it can reach. In step iv), the second user device 2 then connects to the network going using the identifier Y of the first user device.

In step v), the network initiates an AKA (with a challenge). This could be any standardized LTE AKA. In step vi), the second user device 2 forwards the challenge to first user device 1. The first user device 1 calculates the response and sends it to the second user device 2 which forwards it to the network in step vii). The network compares the response to the expected response and provides an OK to the second user device 2 which forwards it to the first user device 1 in step viii). Steps v)-viii) may be omitted in cases wherein security contexts can be stored, such as in LTE. The keys are stored in the network and no full AKA is necessary. In that case, the steps 5-8 can be omitted. Such an example is provided in Fig. 7.

In step ix), the first user device 1 provides a set of keys to the second user device 2. These keys may e.g. contain the user plane key K_{UP} and the radio resource key K_{RRC}. With these two keys, the second user device 2 can decrypt and insert the user plane traffic and behave properly on the radio channel as long as it remains in reach of one eNodeB in the E-UTRAN.

For hand-overs, etc. (which require a key on a higher level) the second user device 2 may consult the first user device 1 for all the procedures. For session management, which require non-access stratus keys K_{NAS}, the second user device 2 also relies on the first user device 1. In this manner, the first user device 1 remains in control of the connection and can quickly disable the second user device 2 if necessary or desired.

The first user device 1 may indicate whether there is some application traffic that it would like to receive and request that the second user device 2 forwards it to the first user device 1. The second user device 2 may forward at least the NAS signaling to the first user device 1 (the second user device 2 itself has not obtained the NAS keys). The connection may be terminated by the first user device 1 by initiating a key refresh procedure, thereby invalidating the keys provided to the second user device 2.

Figs. 8A and 8B schematically illustrate in a different representation than Figs. 5-7 how control is maintained with the first user device 1 while providing a part of the credential information to the second user device 2.

Fig. 8A illustrates the case prior to handing over some of the credential from the first user device 1 to the second user device 2. User data is transferred from the first user device 1 over a connection I to the radio network and further to a content network over connection II to a content network and then further over connection III, if necessary. Signaling traffic is conveyed over connections I and IV for session handling to the MME making up a logical connection V illustrated by the dashed arrow.

Fig. 8B is the illustration after transferring a part of the credentials to the second user device 2 over connection VI. User data is transferred from the second user device 2 over connection VII (and maybe over connection VI) to the radio network and then further over connections II and III. Signaling traffic is now over connections VI, VII and IV, still making up for logical connection V. Accordingly, control remains with the first user device 1 since the first user device 1 can decide to render the credentials provided to the second user device 2 invalid and stop the session. If the direct connection between the first user device 1 and the second user device 2 is blocked, for some reason, the connection of the second user device 2 will fail as soon as a new key should be derived or when the network terminates the connection e.g. because session management errors occur.

The amount and/or type of credentials provided from the first user device 1 to the second user device 2 can vary from only few to the complete set.

In the embodiment of Fig. 9, only the user plane key K_{UP} is provided to the second user device 2.

When proximity is detected by the first user device 1 and the second user device 2, a direct connection is established. In step i), the second user device 2 requests a data session to the network from the first user device 1. The first user device 1 establishes a session with the network if such a session is not yet in existence. In step ii), the first user device informs the second user device 2 that it would like to talk directly to its base band processor 22 (see Fig. 1). Additionally, the first user device 1 informs the second user device 2 how to insert the user data and provides the user plane key K_{UP} to the second user device 2. At a specified point in time, the second user device 2 takes over the radio connection and

the first user device 1 talks to the base band processor directly and informs the second user device 2 where to insert user data traffic.

Because the first user device 1 talks directly to the base band processor 22 of the second user device 2, the first user device 1 does all the signaling (access stratum and non-access stratum). The second user device 2 inserts the user plane traffic straight away. Handovers to GSM or UMTS require that either the first user device 1 gives the newly derived keys to the second user device 2 and lets the second user device 2 handle the session or that the first user device 1 handles all the traffic itself and that the user data flows over the direct connection (so from the second user device 2 to the first user device 1 to the network).

Instead of only providing a single key to the second user device 2, as described with reference to Fig. 9, the complete set of obtained credentials may be provided from the first user device 1 to the second user device 2. Control by the first user device 1 is obtained by informing the network that one or more of the credentials provided to the second user device 2 should no longer be accepted. Various examples of such an embodiment will now be described with reference to Figs. 10-12.

In FIG. 10 it is assumed that the first user device 1 and the second user device 2 are nearby and have paired at some time t_0 and have established a direct connection. At some later time $t_1 = t_0 + dt$, the first user device 1 would like to go into battery saving mode or forward an ongoing call to the nearby second user device 2. The first user device 1 informs the network in step i) that it would like to connect through the second user device 2. The network provides the first user device 1 with a full set of credentials comprising a temporary identifier X and a key or keys or key identifier(s) Y in step ii). The first user device 1 provides the second user device 2 with the identifier X and the key and the identifier of the network it can reach in step iii).

The second user device 2 then connects to the network in step iv) using the credentials received from the first user device 1 and performs a full AKA, steps v)- vii), in a known manner. The second user device 2 has the complete set of credentials and can perform all management functions on its own. The first user device 1 may hand over a session to the second user device 2. Control, however, may still be exercised from the first user device 1, knowing the credentials of the second user device 2, by connecting to the network and signaling, using information relating to the credentials provided to the second user device 2, that the second user device 2 should be connected. The second user device 2 may save the security context when it detaches from the network (step viii)) and attach again (steps ix) and x)) at a later time as long as the first user device 1 has not instructed the network otherwise.

Further embodiments are disclosed in Figs. 11 and 12. In both embodiments, the first user device 1 and second user device 2 device are paired at some time t_0 and have setup a direct connection. At some later time $t_1 = t_0 + dt$, the first user device 1 would like to go into battery saving mode or forward an ongoing call to the nearby second user device 2. The first user device 1 informs the network that it would like to connect through the second user device 2 device in step i). The network provides the first user device 1 device with an identifier X in step ii). Then, in steps iii)- viii) for Fig. 11 and in steps iii)- vi) for Fig. 12 an AKA is performed by the first user device 1 (either relayed through the second user device as in Fig. 11) or by the first user device 1 itself (as illustrated in Fig. 12).

When the keys are obtained, the first user device 1 provides the keys to the second user device 2 in step ix) (Fig. 11) and in step vii) (Fig. 12). In the example of Fig. 12, also the identifier is provided to the second user device 2. Again, by saving the security context, the second user device 2 may detach and attach again as long as the first user device 1 has not informed the network that the second user device 2 should not be allowed to connect anymore.

In an alternative to the above solutions, the first user device 1 may obtain the credentials independent of whether it has a connection to a second user device 2. The first user device 1 could for example obtain multiple full credential sets in advance and use these whenever needed. Similarly, the network and first user device 1 could agree a shared secret / key that the first user device 1 could use for deriving new sets of credentials in the first user device 1. In that case, the shared secret will provide proof of origin of the set of credentials (only the network and first user device 1 know the shared secret so any third device should have got it from the first user device 1). Such information could also be contained in a certificate which could be provided by the first user device 1 to the second user device 2 upon attach of the second user device 2.

The second user device 2 may be instructed to listen for the identifier that has been given to it before in order to setup a direct connection between the second user device 2 and first user device 1 (the first user device 1 would then be broadcasting this identifier). When the first user device 1 and the second user device 2 find themselves at a greater distance, the broadcast by the first user device 1 could propagate through the operator network and the second user device 2 device could connect to the cellular network (or only the radio / access network) and set up a device-to-device connection. An additional requirement would be that the network knows where to page the second user device 2, either because it has a static location, or because the second user device 2 device keeps the network or the user device 1 informed.

Advantageously, there is no need for a separate subscription for every device and all devices could be managed from one device (or multiple in case it is a family owned device). So, if a household has four members and four subscriptions, there are four devices potentially capable of controlling the in-house entertainment system, photo camera or game console.

For solutions where a full credential set is provided to the second user device 2, there is no need for special arrangements for changing coverage. Moving between LTE, UMTS and GSM coverage is seamlessly possible because the set is full and therefore all standard procedures for hand-overs apply.

In some of the disclosed embodiments where not all information is provided to the second user device 2, the first user device 1 informs the second user device 2 about the channels (e.g. frequencies) that are to be used and the time slots that are available for sending information. The second user device 2 then has all information to be able to effectively eavesdrop on the connection it is relaying or repeating.

In some embodiments, the control by the first user device 1 is performed by keeping the signaling on the first user device 1 and only working with the user data on the second user device 2. That way, the first user device 1 can effectively control by initiating a key refresh procedure. Another point of

added security is that the session signaling remains between the first user device 1 and the network. Thereby, the first user device 1 can control the properties of the session, such as maximum allowed throughput and QoS aspects. The first user device 1 retains (some) control of what is allowed for the session (no large downloads, e.g.).

The disclosed control mechanisms can be used for privacy enhancing technology. For example, medical devices, such as a pacemaker, a blood pressure monitoring device, blood sugar level monitoring device, etc. could use this technology to push information to the network. In this case, the health care device (a second user device) could not have a subscription, but it is paired with a phone (a first user device). At some point, the health care device would like to send information to the health care provider. The medical device then pages the phone (to see whether it is nearby). If the phone receives the paging message it replies and a direct connection is set up. Then, the medical device indicates that it would like to connect to the network to send some data. The phone then can decide whether to allow or not and whether or not to allow the device to send the information.

As mentioned previously, the disclosed control mechanism has been envisaged for a variety of networks, including LTE (4G) networks and UMTS networks. At present, a next generation network intended to succeed the LTE network is under development. One aspect distinguishing the next generation network from the LTE network is the further separation of user plane data and signaling plane data.

Fig. 13 represents an envisioned key hierarchy for a next generation network resembling the EPS key hierarchy. The key hierarchy has large similarity to the LTE key hierarchy as depicted in Fig. 4, but has a further key division for the UE-eNodeB radio interface. In particular, the user plane key K_{UP} may be assigned to a single eNodeB and a single data session by using an intermediate key (e.g. a session identifier) from which multiple user plane keys K'_{UPenc} are derived.

This enables the first user device 1 to have a direct (physical) signaling connection with the network and the second user device 2 to have a direct (physical) user data connection as depicted in Fig. 14. The signaling connection may comprise a low bandwidth channel and the user data connection may comprise a channel with a higher bandwidth. Control of the user data exchange of the second user device 2 may be performed by the first user device 1 manipulating the signaling information or the transmission thereof.

The direct connection between the first user device 1 and the second user device 2 enables the first user device 1 to perform the signaling for the resources and the session and to inform the second device 2 about the timing for the user data transmission and other events on the radio path. If a session identifier is used for deriving the user plane keys K_{UP}, both the first user device 1 and the second user device 2 may have a session with the network. The first user device 1 may then exercise dual session management control functions, both for itself and for the second user device 2. In Fig. 14, the first user device 1 only provided the user plane key to the second user device 2.

The enhanced separation of the user plane and signaling plane makes it possible to use different identifiers for the user plane and the signaling plane. For example, identifiers may be derived

from the TMSI (used for the signaling) and the session identifier using a hash function. This is also a scalable solution since every data connection obtains an associated identifier in this manner.

It is noted that the method has been described in terms of steps to be performed, but it is not to be construed that the steps described must be performed in the exact order described and/or one after another. One skilled in the art may envision to change the order of the steps and/or to perform steps in parallel to achieve equivalent technical results.

With some modifications, one skilled in the art may extend the embodiments described herein to other architectures, networks, or technologies.

Various embodiments of the invention may be implemented as a program product for use with a computer system or a processor, where the program(s) of the program product define functions of the embodiments (including the methods described herein). In one embodiment, the program(s) can be contained on a variety of non-transitory computer-readable storage media (generally referred to as "storage"), where, as used herein, the expression "non-transitory computer readable storage media" comprises all computer-readable media, with the sole exception being a transitory, propagating signal. In another embodiment, the program(s) can be contained on a variety of transitory computer-readable storage media. Illustrative computer-readable storage media include, but are not limited to: (i) non-writable storage media (e.g., read-only memory devices within a computer such as CD-ROM disks readable by a CD-ROM drive, ROM chips or any type of solid-state non-volatile semiconductor memory) on which information is permanently stored; and (ii) writable storage media (e.g., flash memory, floppy disks within a diskette drive or hard-disk drive or any type of solid-state random-access semiconductor memory) on which alterable information is stored.

It is to be understood that any feature described in relation to any one embodiment may be used alone, or in combination with other features described, and may also be used in combination with one or more features of any other of the embodiments, or any combination of any other of the embodiments. Moreover, the invention is not limited to the embodiments described above, which may be varied within the scope of the accompanying claims.

CLAIMS

1. A method for controlling, by a first user device, user data exchange of a second user device over a telecommunications network, wherein the first user device and the second user device are configured for wirelessly connecting to the telecommunications network, the method comprising the steps of:
   - obtaining a set of credentials by the first user device, the set of credentials comprising an identifier and a plurality of signal transmission keys for signal transmission over the telecommunications network;
   - providing at least a portion of the set of credentials from the first user device to the second user device to enable the second user device to exchange user data over the telecommunications network;
   - controlling user data exchange of the second user device over the telecommunications network by means of a control action of the first user device, the control action being performed with respect to the credentials obtained by the first user device and provided to the second user device.

2. The method according to claim 1, wherein the control action comprises at least one of:
   - instructing the telecommunications network to invalidate the identifier if the identifier has been provided to the second user device; and
   - instructing the telecommunications network to invalidate one or more of the keys that have been provided to the second user device.

3. The method according to claim 1, wherein only a portion of the set of credentials is provided to the second user device and wherein the control action is performed by at least one of:
   - modifying one or more credentials retained in the first user device; and
   - invalidating one or more of the credentials provided to the second user device.

4. The method according to claim 3, wherein the signal transmission keys are organized in a key hierarchy and wherein a key lower in the key hierarchy is derived from a key higher in the key hierarchy and the first user device provides one or more signal transmission keys lower in the key hierarchy to the second user device while retaining one or more signal transmission keys higher in the key hierarchy, the control action comprising generating new keys for one or more of the signal transmission keys higher in the key hierarchy.

5. The method according to claim 3, wherein the signal transmission keys provided by the first user device to the second user device only includes a user plane encryption key, the method further comprising the steps of:
   - providing user data inclusion details to the second user device;

- controlling user data exchange for the second user device in dependence of one or more of the credentials remaining in the first user device.

6. The method according to claim 1, further comprising the step of maintaining signalling between the first user device and the telecommunications network for the user data exchange of the second user device over the telecommunications network and wherein the control action by the first user device comprises manipulating the signalling at the first user device.

7. The method according to claim 6, wherein the telecommunications network comprises an LTE network and the set of credentials obtained by the first user device includes one or more non-access stratum (NAS) keys, the method comprising the steps of:
- omitting one or more of the NAS keys from the portion of the credentials provided to the second user device;
- aborting user data exchange of the second user device by the control action, the control action of the first user device comprising one of:
    - transmitting a NAS message Detach Request to the telecommunications network;
    - transmitting an authentication failure message upon receiving a challenge from the telecommunications network during a Tracking Area Update (TAU) or an Authentication and Key Agreement procedure.

8. The method according to claim 1, further comprising the steps of:
- applying a first identifier from the telecommunication network enabling the first user device to exchange user data over the telecommunications network;
- requesting a second identifier from the telecommunications network;
- including the second identifier in the set of credentials to be provided to the second user device to enable the second user device to exchange user data over the telecommunications network.

9. The method according to claim 1, comprising the step of receiving an identifier enabling the first user device to exchange user data over the telecommunications network and providing this identifier to the second user device enabling the second user device to exchange user data over the telecommunications network.

10. The method according to one or more of the preceding claims, further comprising the step of establishing a direct connection, such as an LTE direct connection or a Bluetooth connection, between the first user device and the second user device for at least providing the at least portion of the set of credentials to the second user device.

11. The method according to one or more of the preceding claims, wherein the first user device obtains one or more sets of credentials in advance and provides one or more of the sets of credentials to one or more second user devices at a later time.

12. The method according to one or more of the preceding claims, comprising the steps by the first user device of:
- providing the identifier to the second device;
- receiving information from the telecommunications network via the second user device;
- transmitting one or more signal transmission keys to the second device after receiving the information from the second device.

13. A computer program comprising software code portions configured for, when executed on a computer system, performing the method according to one or more of the claims 1-12.

14. A non-transitory computer program medium comprising the computer program according to claim 13.

15. A first user device configured for executing the method according to claims 1-12 and comprising circuitry programmed with computer code for controlling user data exchange by the second user device, wherein the computer code, when executed by the circuitry, performs:
- obtaining a set of credentials, the set of credentials comprising an identifier and a plurality of signal transmission keys for signal transmission over the telecommunications network;
- providing at least a portion of the set of credentials to the second user device to enable the second user device to exchange user data over the telecommunications network;
- controlling user data exchange of the second user device over the telecommunications network by means of a control action, the control action being performed with respect to the obtained credentials provided to the second user device.

16. A second user device configured for being controlled by a first user device according to the method of claims 1-12, the second user device comprising circuitry programmed with computer code for being controlled by the first user device according to claim 15.

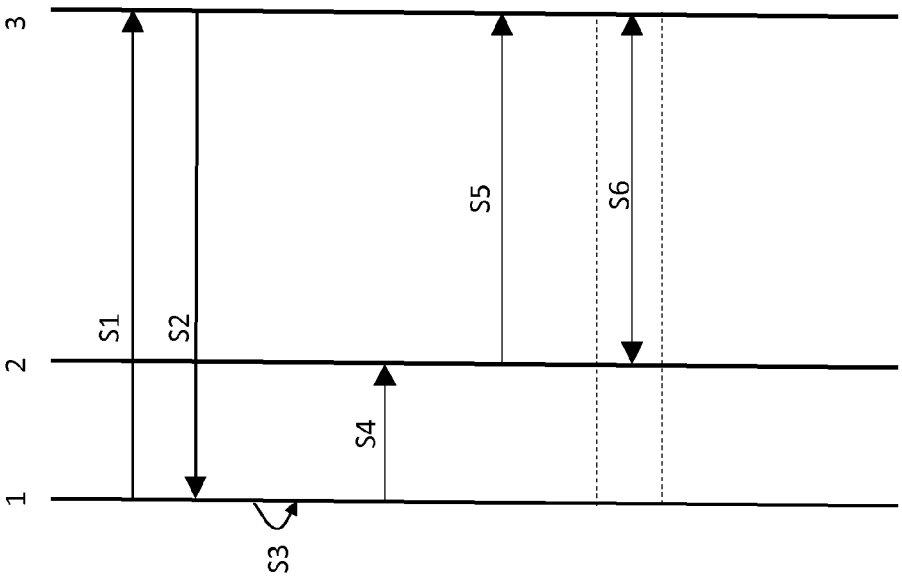

FIG. 2

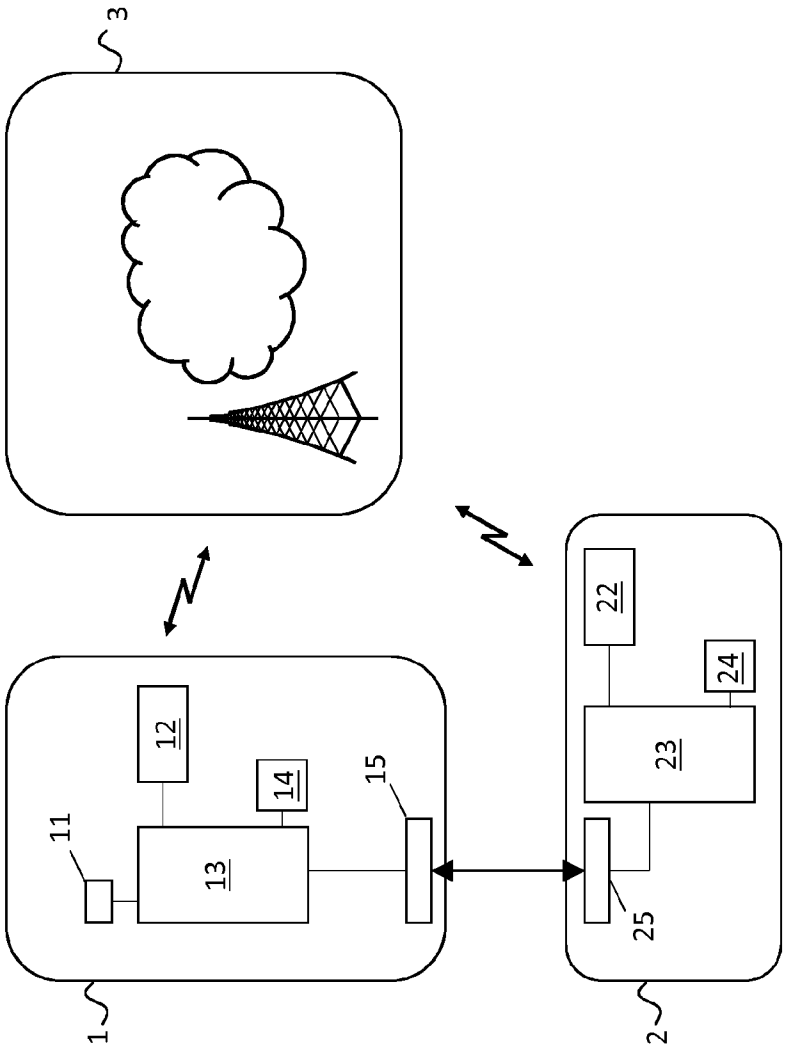

FIG. 1

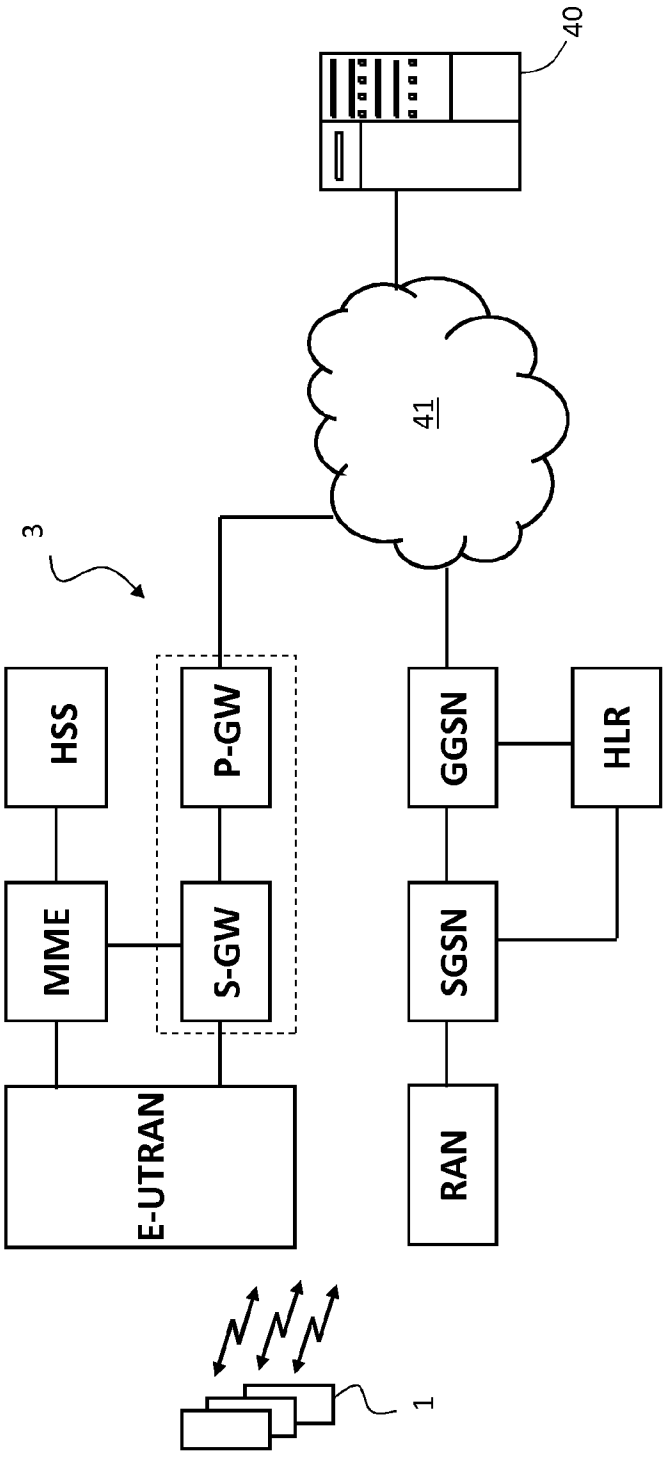

FIG. 3

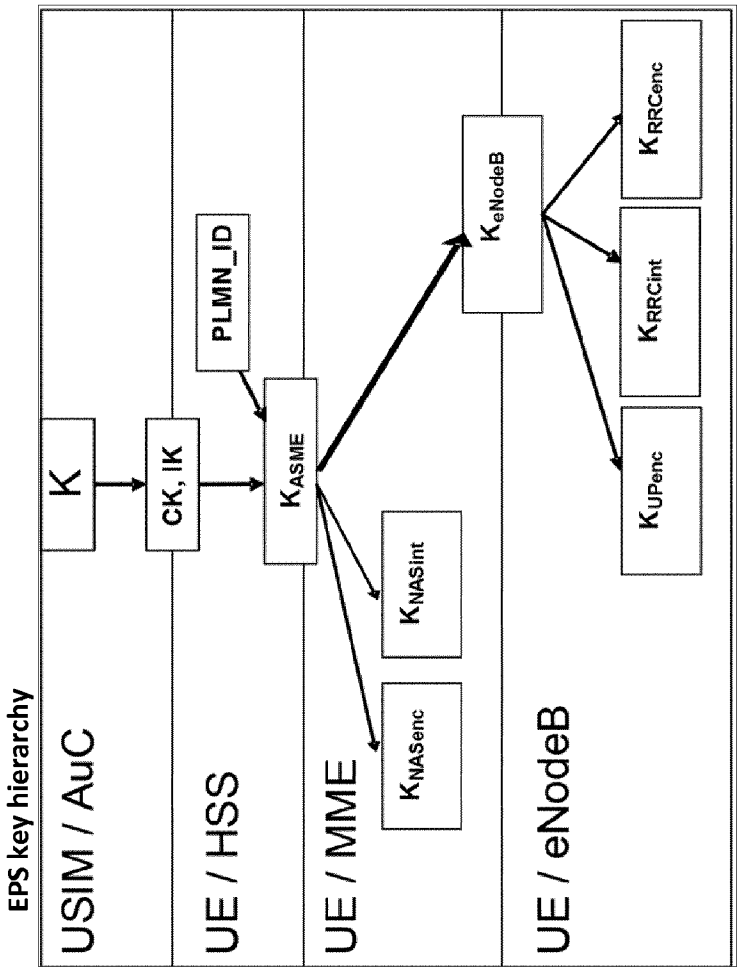
EPS key hierarchy
USIM / AuC
UE / HSS
UE / MME
UE / eNodeB
K
CK, IK
PLMN_ID
KASME
KNASint
KNASenc
KeNodeB
KRRCenc
KRRCint
KUPenc

FIG. 4

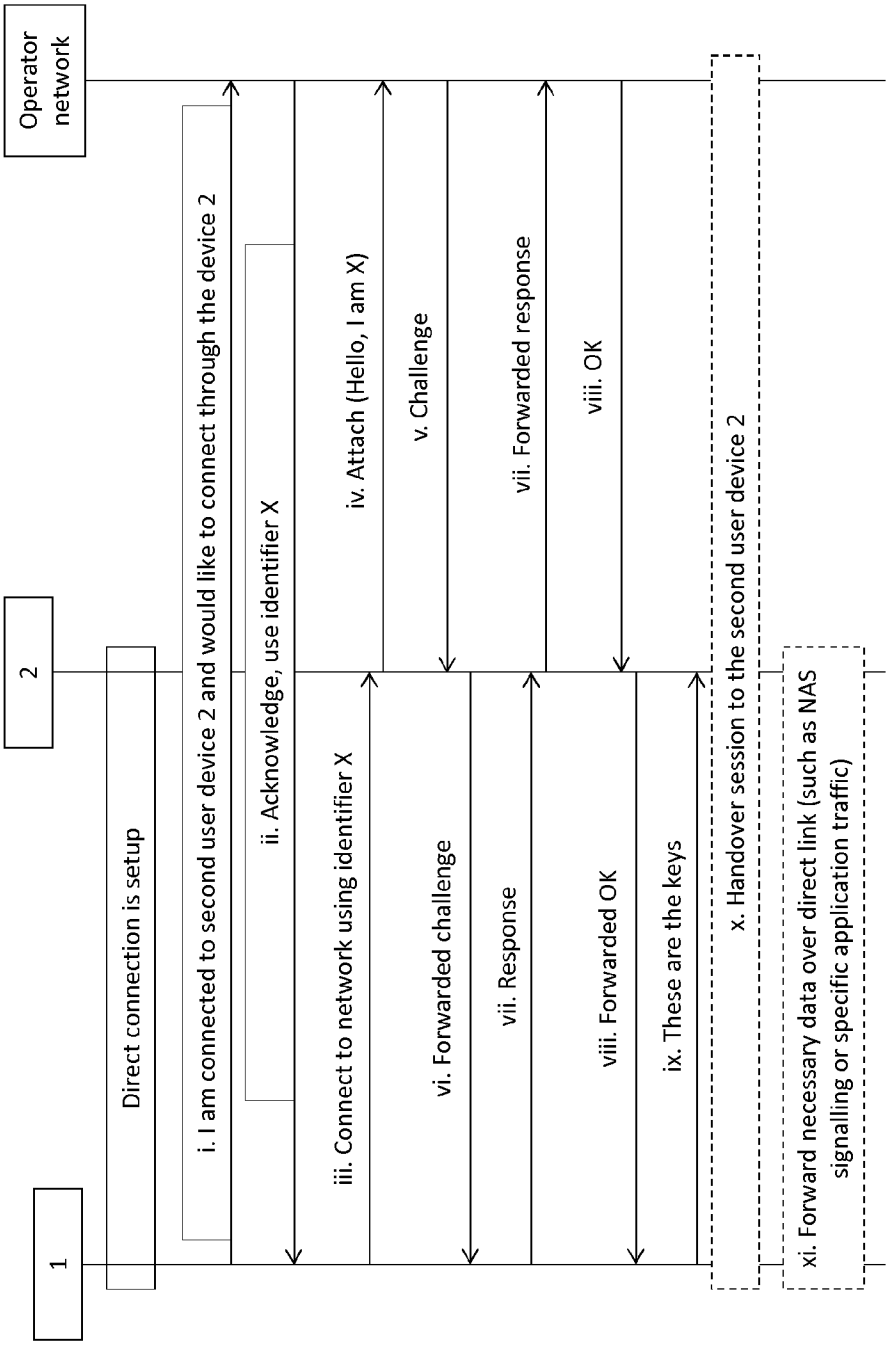
Operator network
2
1
Direct connection is setup
i. I am connected to second user device 2 and would like to connect through the device 2
ii. Acknowledge, use identifier X
iii. Connect to network using identifier X
iv. Attach (Hello, I am X)
v. Challenge
vi. Forwarded challenge
vii. Response
vii. Forwarded response
viii. OK
viii. Forwarded OK
ix. These are the keys
x. Handover session to the second user device 2
xi. Forward necessary data over direct link (such as NAS signalling or specific application traffic)

FIG. 5

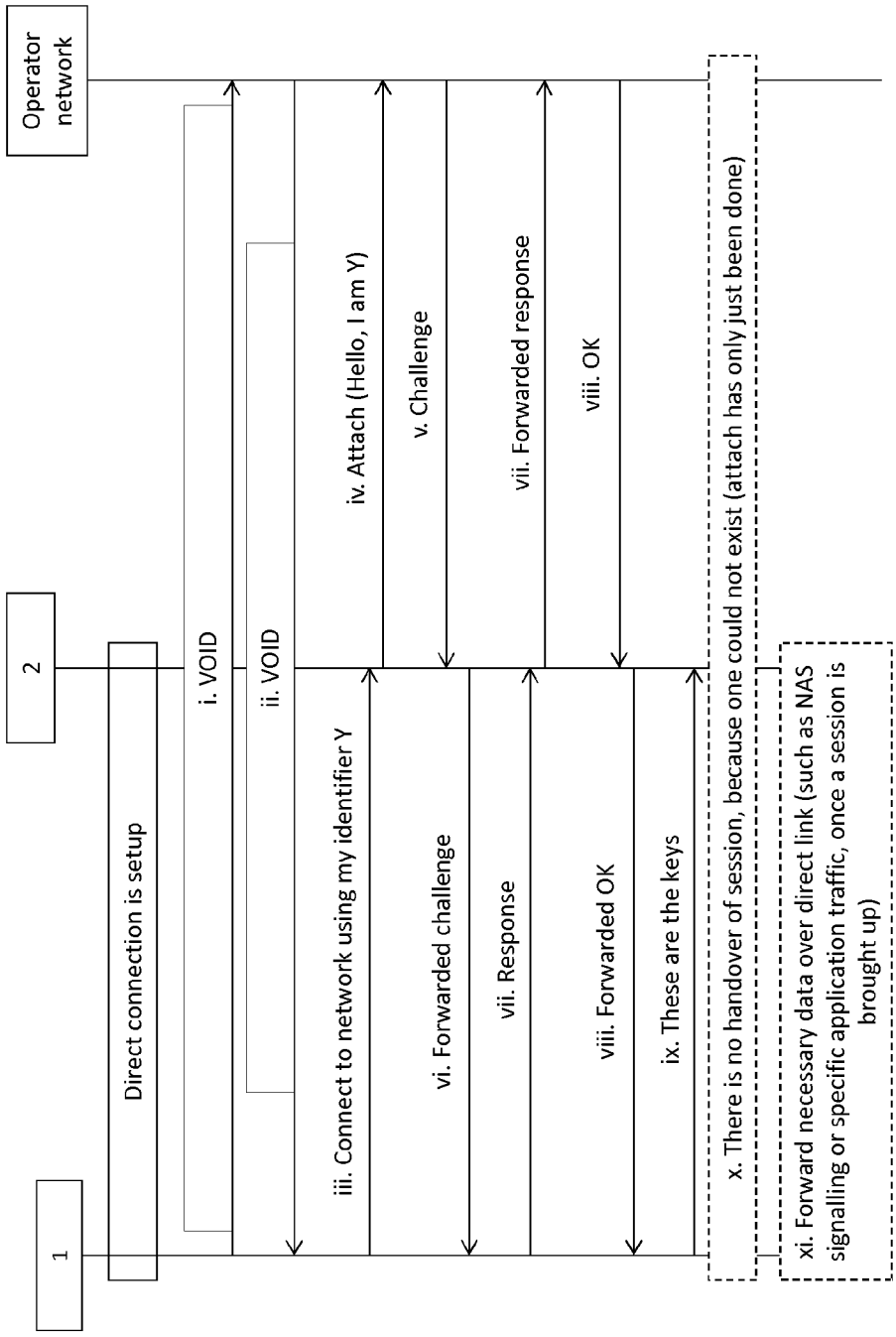
Operator network
2
1
Direct connection is setup
i. VOID
ii. VOID
iii. Connect to network using my identifier Y
iv. Attach (Hello, I am Y)
v. Challenge
vi. Forwarded challenge
vii. Response
vii. Forwarded response
viii. OK
viii. Forwarded OK
ix. These are the keys
x. There is no handover of session, because one could not exist (attach has only just been done)
xi. Forward necessary data over direct link (such as NAS signalling or specific application traffic, once a session is brought up)

FIG. 6

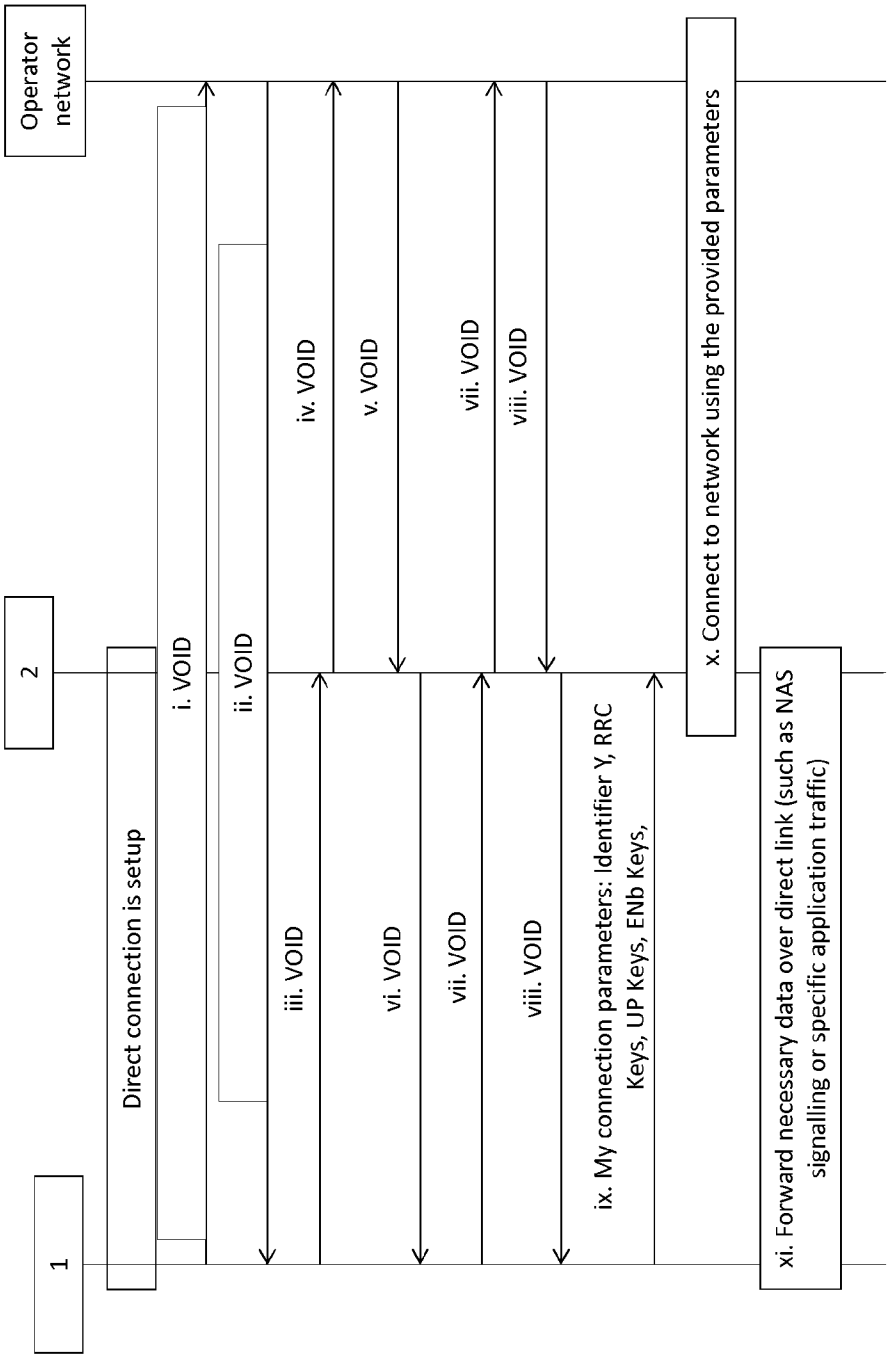
Operator network
2
1
Direct connection is setup
i. VOID
ii. VOID
iii. VOID
iv. VOID
v. VOID
vi. VOID
vii. VOID
viii. VOID
ix. My connection parameters: Identifier Y, RRC Keys, UP Keys, ENb Keys,
x. Connect to network using the provided parameters
xi. Forward necessary data over direct link (such as NAS signalling or specific application traffic)

FIG. 7

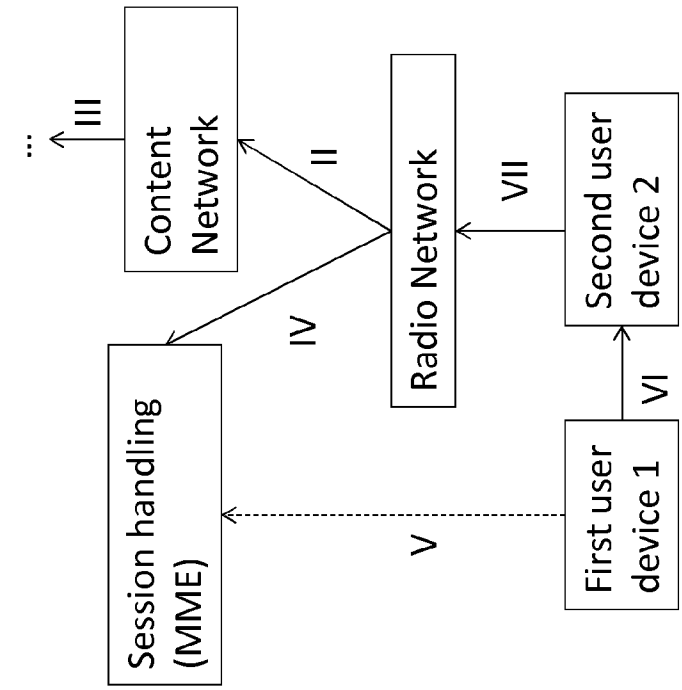
Content Network
Radio Network
Second user device 2
Session handling (MME)
First user device 1
III
II
VII
IV
VI
V

FIG. 8B

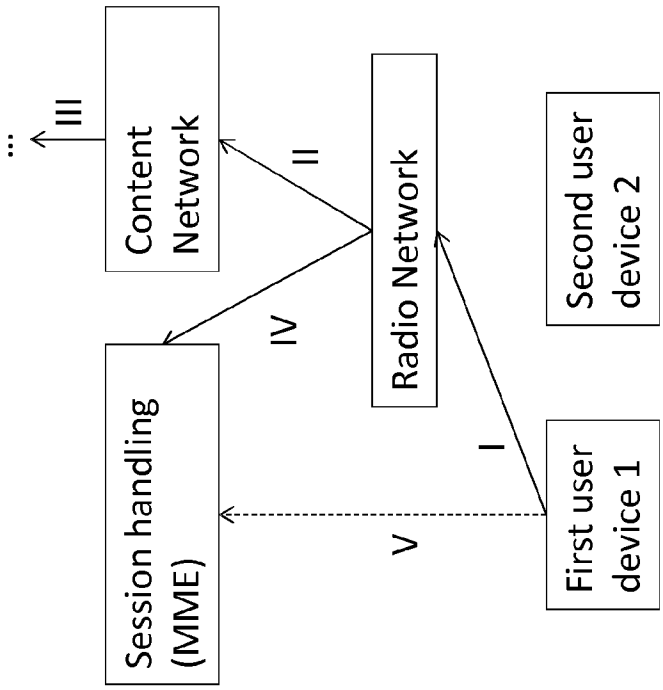
Content Network
Radio Network
Second user device 2
Session handling (MME)
First user device 1
III
II
IV
I
V

FIG. 8A

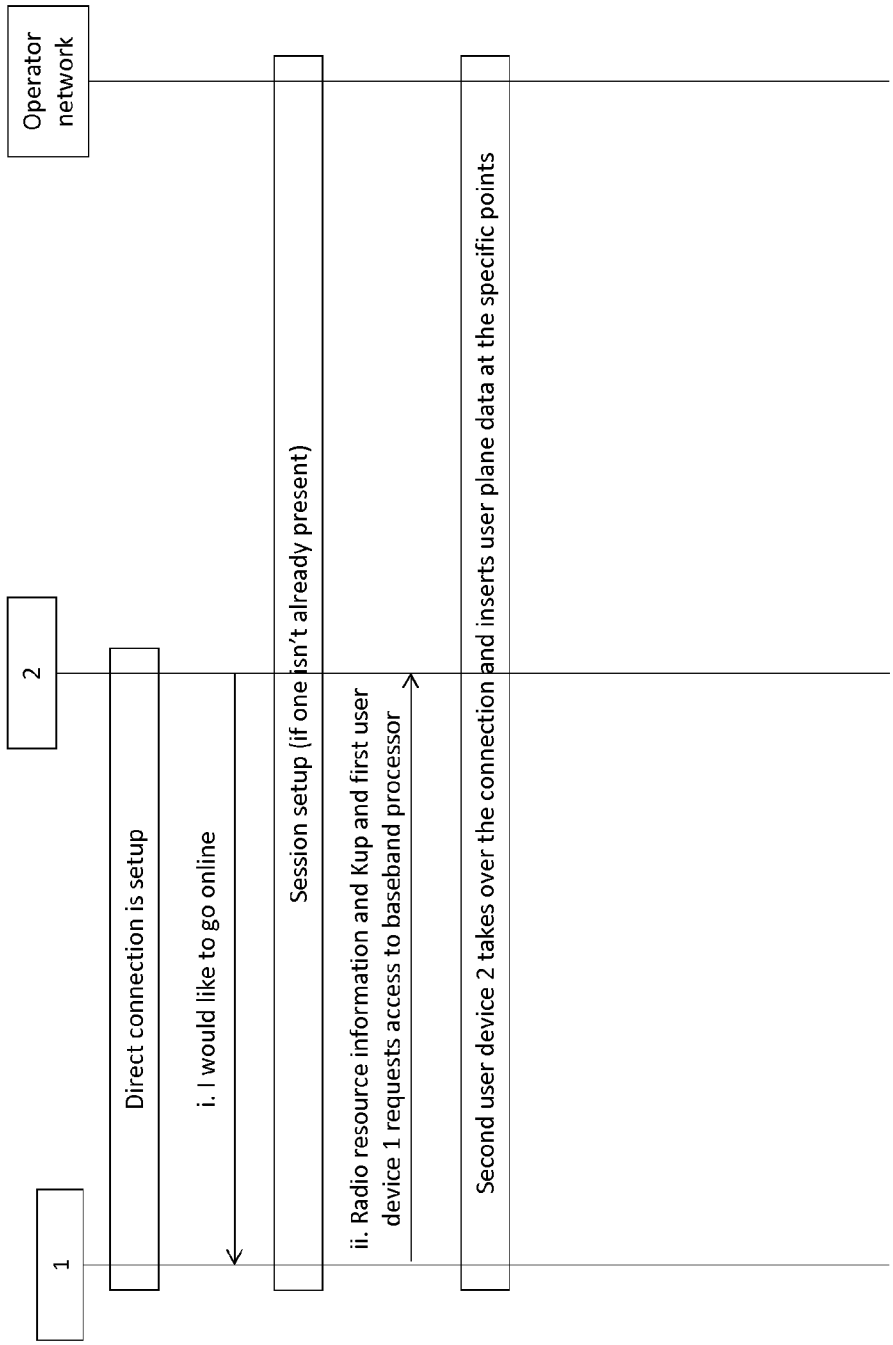
Operator network
2
1
Direct connection is setup
i. I would like to go online
Session setup (if one isn't already present)
ii. Radio resource information and Kup and first user device 1 requests access to baseband processor
Second user device 2 takes over the connection and inserts user plane data at the specific points

FIG. 9

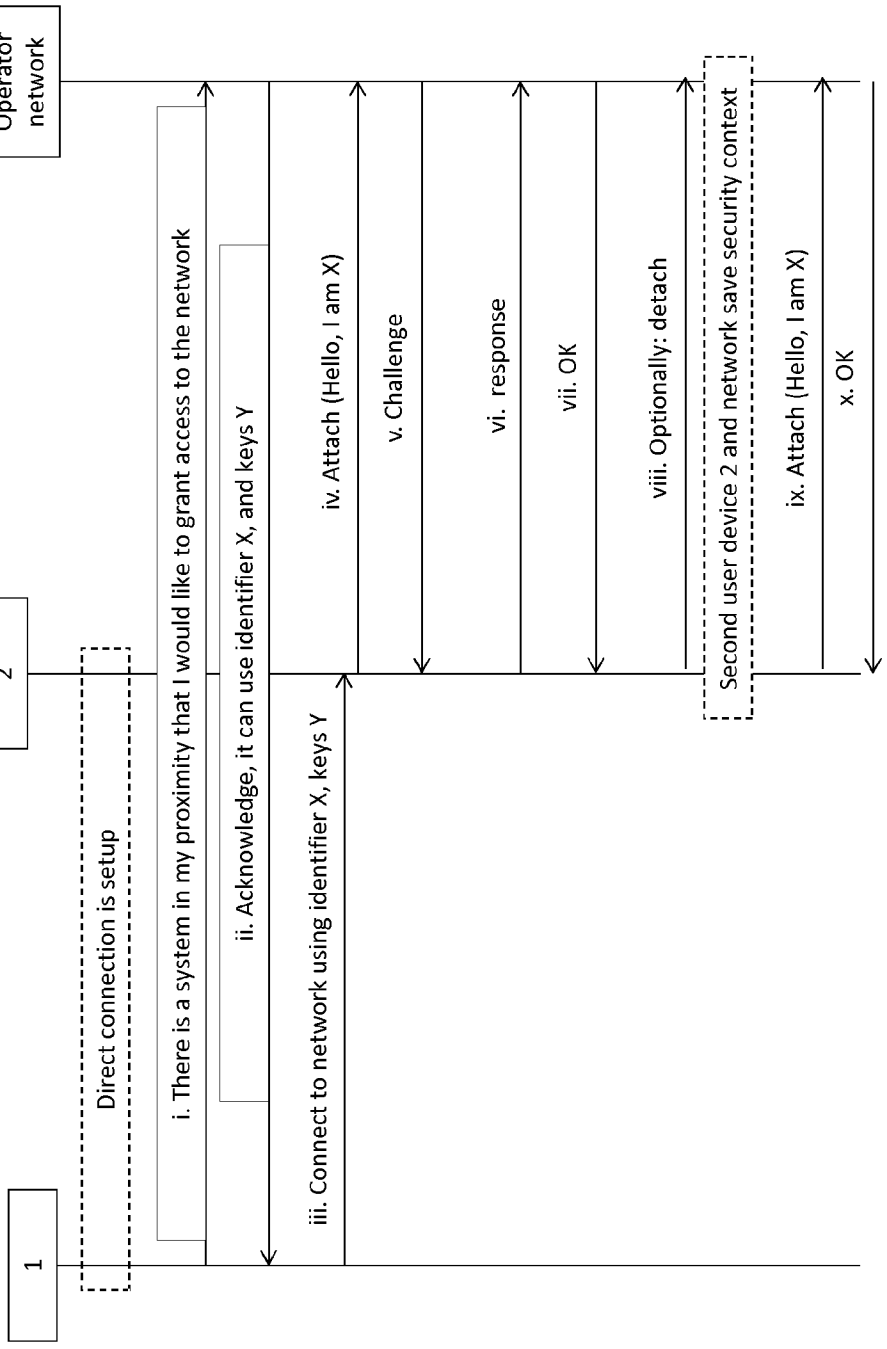
Operator network
2
1
Direct connection is setup
i. There is a system in my proximity that I would like to grant access to the network
ii. Acknowledge, it can use identifier X, and keys Y
iii. Connect to network using identifier X, keys Y
iv. Attach (Hello, I am X)
v. Challenge
vi. response
vii. OK
viii. Optionally: detach
Second user device 2 and network save security context
ix. Attach (Hello, I am X)
x. OK

FIG. 10

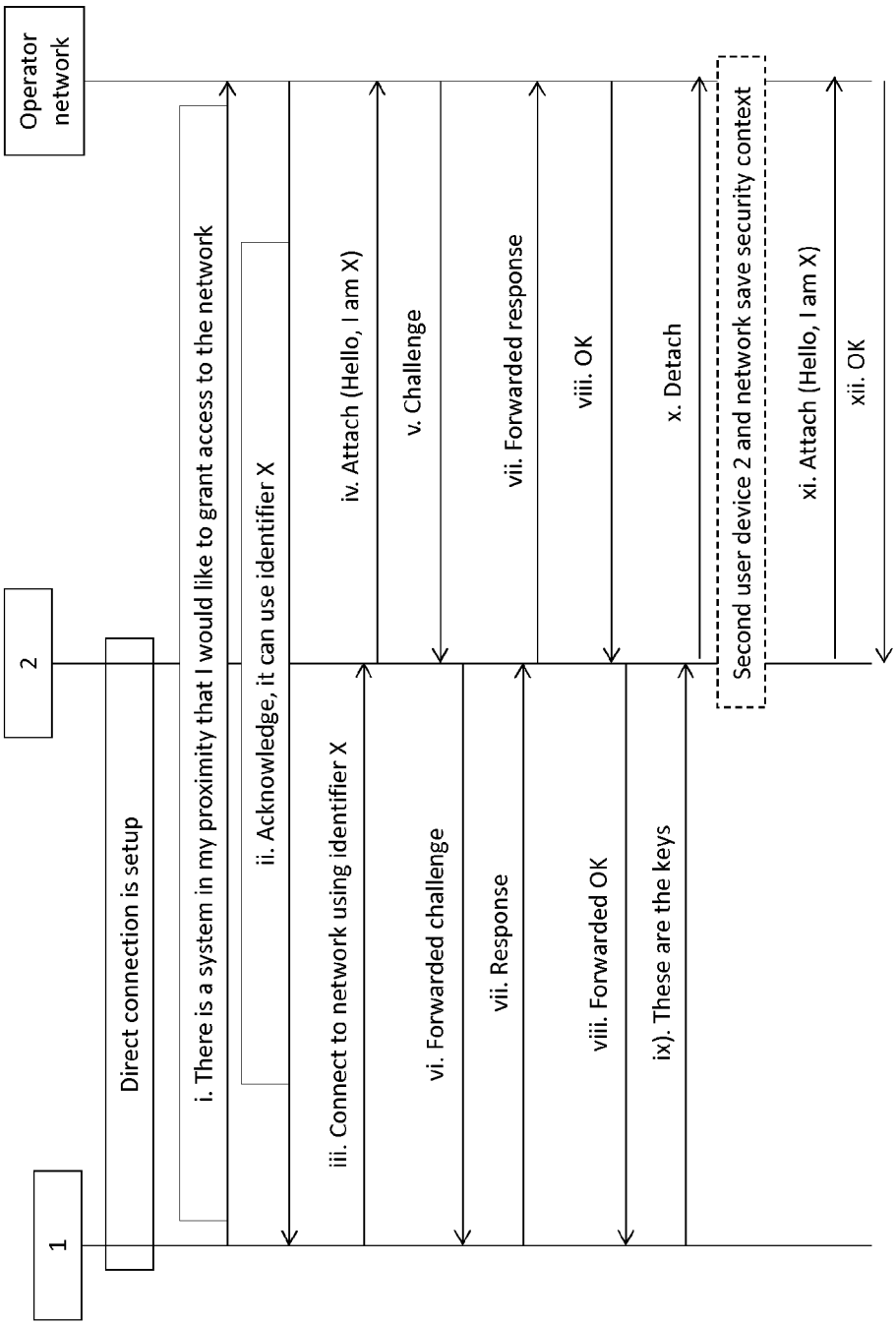
Operator network
2
1
Direct connection is setup
i. There is a system in my proximity that I would like to grant access to the network
ii. Acknowledge, it can use identifier X
iii. Connect to network using identifier X
iv. Attach (Hello, I am X)
v. Challenge
vi. Forwarded challenge
vii. Response
vii. Forwarded response
viii. Forwarded OK
viii. OK
ix). These are the keys
x. Detach
Second user device 2 and network save security context
xi. Attach (Hello, I am X)
xii. OK

FIG. 11

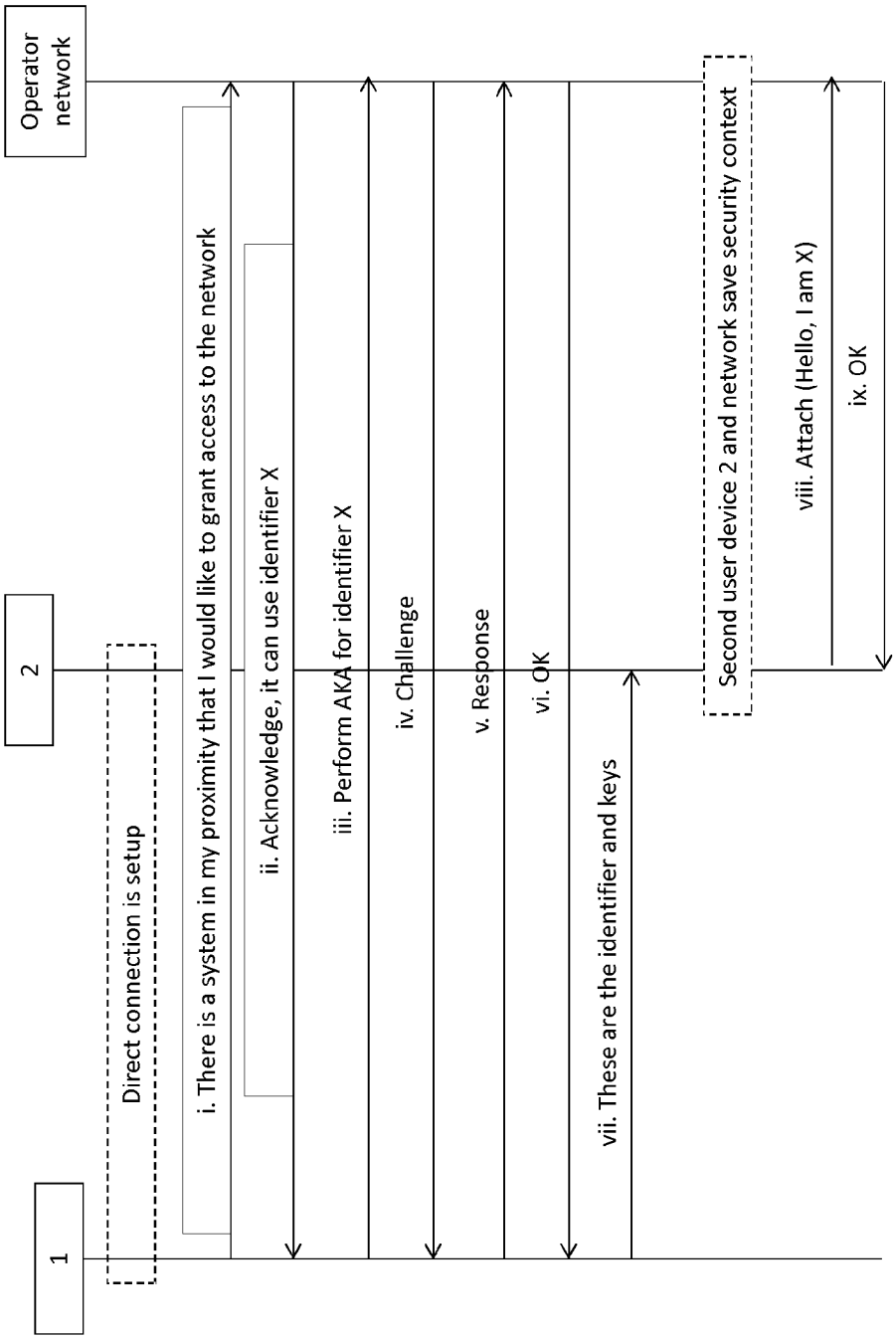
Operator network
2
1
Direct connection is setup
i. There is a system in my proximity that I would like to grant access to the network
ii. Acknowledge, it can use identifier X
iii. Perform AKA for identifier X
iv. Challenge
v. Response
vi. OK
vii. These are the identifier and keys
Second user device 2 and network save security context
viii. Attach (Hello, I am X)
ix. OK

FIG. 12

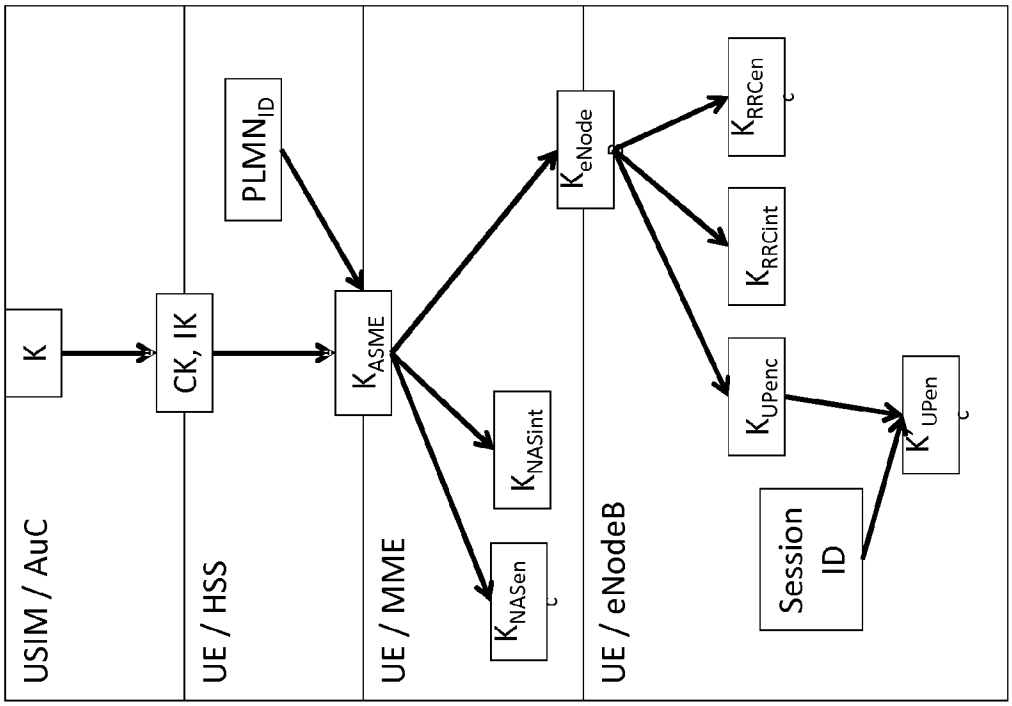
USIM / AuC
UE / HSS
UE / MME
UE / eNodeB
K
CK, IK
PLMN_ID
K_ASME
K_NASint
K_NASenc
K_eNodeB
K_RRCenc
K_RRCint
K_UPenc
Session ID
K_UPenc

FIG. 13

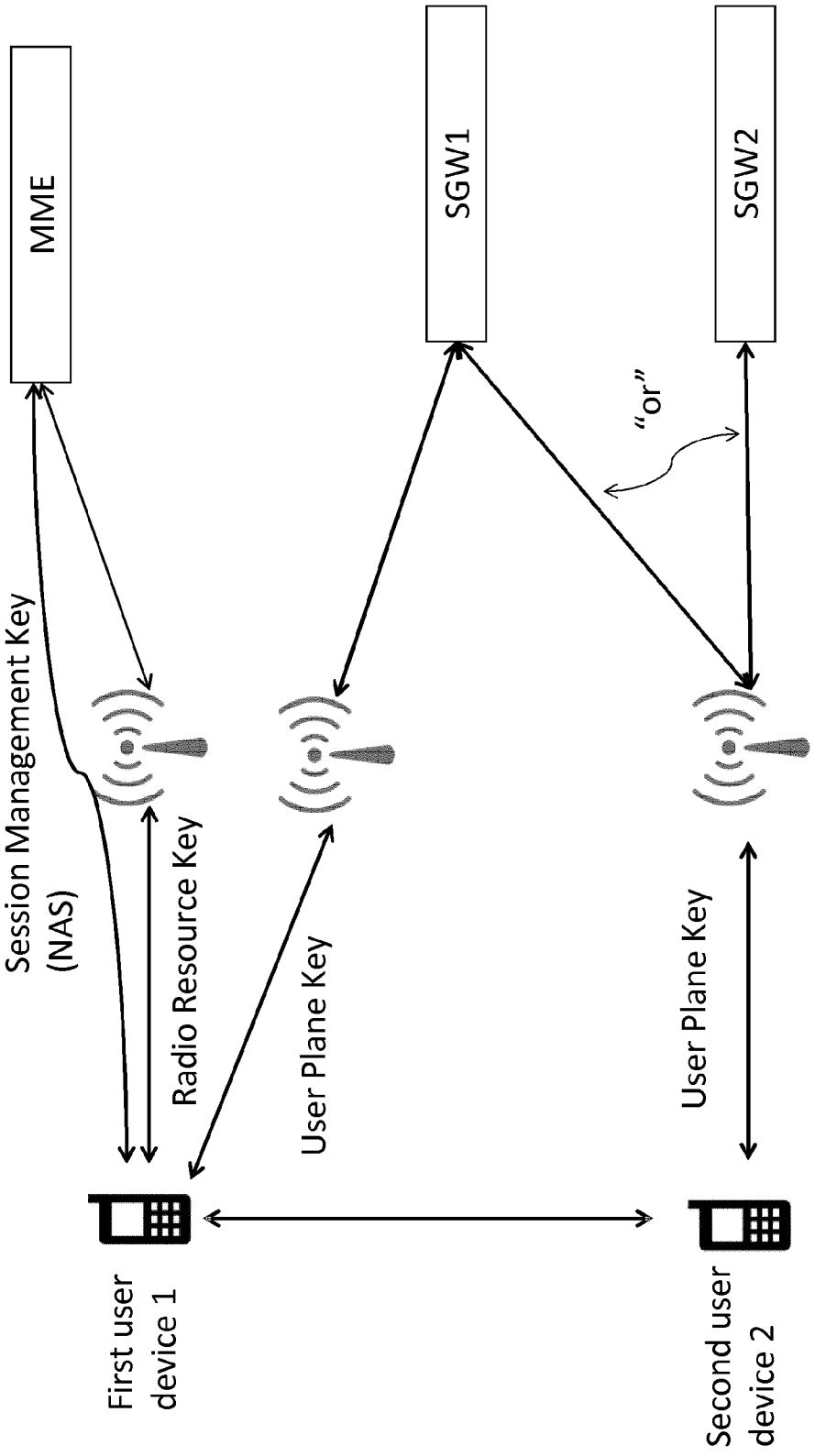
MME
SGW1
SGW2
"or"
Session Management Key (NAS)
Radio Resource Key
User Plane Key
User Plane Key
First user device 1
Second user device 2

FIG. 14

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2014/072874

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06 H04W12/04 H04L9/08
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)
H04L H04W

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

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2002/169966 A1 (NYMAN KAI [FI] ET AL) 14 November 2002 (2002-11-14) paragraph [0022] - paragraph [0028]; figures 1-2 paragraph [0093] - paragraph [0102]	1-16
X	US 2012/047551 A1 (PATTAR SUDHIR B [US] ET AL) 23 February 2012 (2012-02-23) paragraph [0003] - paragraph [0006]; figures 3, 10-12 paragraph [0038] - paragraph [0050] paragraph [0080] - paragraph [0097]	1-16
X	DE 100 12 057 A1 (BOSCH GMBH ROBERT [DE]) 20 September 2001 (2001-09-20) abstract; figure 1 column 4, line 16 - line 19 column 4, line 25 - column 5, line 35	1,13-16

-/--

[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
1 December 2014	05/12/2014

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	Figiel, Barbara

1

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2014/072874

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 2012/035335 A1 (VODAFONE IP LICENSING LTD [GB]; BONE NICHOLAS [GB]) 22 March 2012 (2012-03-22) the whole document -----	1-16

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2014/072874

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2002169966 A1	14-11-2002	EP 1397932 A1	17-03-2004
		US 2002169966 A1	14-11-2002
		WO 02093967 A1	21-11-2002
US 2012047551 A1	23-02-2012	CN 102687547 A	19-09-2012
		EP 2520110 A1	07-11-2012
		JP 2013516149 A	09-05-2013
		KR 20120099794 A	11-09-2012
		KR 20140074357 A	17-06-2014
		TW 201141124 A	16-11-2011
		US 2012047551 A1	23-02-2012
		WO 2011082150 A1	07-07-2011
DE 10012057 A1	20-09-2001	DE 10012057 A1	20-09-2001
		FR 2806568 A1	21-09-2001
		GB 2365699 A	20-02-2002
		IT MI20010481 A1	09-09-2002
WO 2012035335 A1	22-03-2012	EP 2617217 A1	24-07-2013
		US 2014150073 A1	29-05-2014
		WO 2012035335 A1	22-03-2012