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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
20 December 2012 (20.12.2012)

WIPO | PCT

(10) International Publication Number
WO 2012/173539 A1

(51) International Patent Classification:
H04W 12/06 (2009.01) *H04W 8/18* (2009.01)
H04L 29/06 (2006.01) *H04W 8/20* (2009.01)

(21) International Application Number:
PCT/SE2011/050759

(22) International Filing Date:
16 June 2011 (16.06.2011)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: **TELEFONAKTIEBOLAGET L M ERICSSON (PUBL)** [SE/SE]; S-164 83 Stockholm (SE).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **MURAKAMI, Shingo** [JP/JP]; C-301, 41 Morinodai, Midori-ku, Yokohama, Kanagawa, Kanagawa 226-0029 (JP). **ODA, Toshikane** [JP/JP]; 3-10-17 Kamiuma, Setagaya-ku, Tokyo, Tokyo 154-0011 (JP). **SUGIMOTO, Shinta** [JP/JP]; 2013, The Kosugi Tower, 13-17, Nakamaruko, Nakahara-ku, Kawasaki-shi, Kanagawa, Kanagawa 211-0012 (JP). **KATO, Ryoji** [JP/JP]; 10-9, Wakamiya-dai, Yokosuka, Kanagawa, Kanagawa 239-0829 (JP).

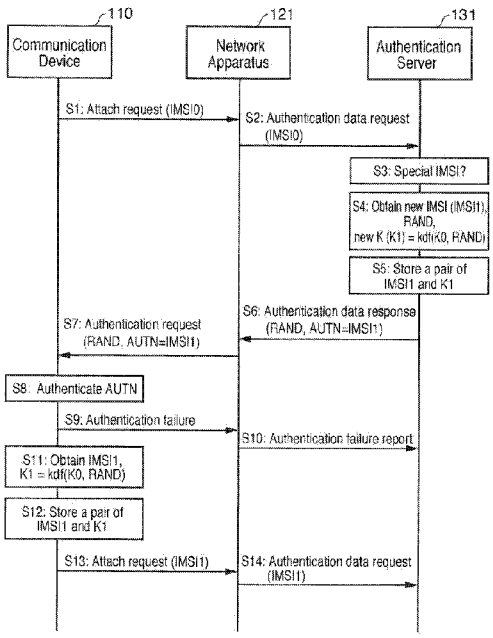
(74) Agent: **NORIN, Klas**; Ericsson AB, Patent Unit SLM, Torshamnsgatan 21-23, S-164 80 Stockholm (SE).

(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, 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, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, 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.

[Continued on next page]

(54) Title: AUTHENTICATION SERVER AND COMMUNICATION DEVICE

FIG. 4



(57) Abstract: There is provided an authentication server. The server includes a receiving unit configured to receive a request from a network apparatus. The request includes a subscription identity. The server further includes a determination unit configured to determine whether the received subscription identity is a predetermined subscription identity and an obtaining unit configured to obtain, when it is determined that the received subscription identity is the predetermined subscription identity, a key and a subscription identity. The key is derived by applying a key derivation function to a random number and a key associated with the predetermined subscription identity. The server further includes a storage unit configured to store the obtained key and the obtained subscription identity and a response unit configured to send a response including the random number and an authentication token to the network apparatus. The authentication token includes the obtained subscription identity.

WO 2012/173539 A1

(84) **Designated States** *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, 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, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *of inventorship (Rule 4.17(iv))*

Published:

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

DESCRIPTION

AUTHENTICATION SERVER AND COMMUNICATION DEVICE

TECHNICAL FIELD

[0001] The present invention generally relates to an authentication server and a communication device.

BACKGROUND

[0002] In the field of the remote subscription management such as MCIM (Machine Communication Identity Module) defined in 3GPP TR 33.812, a registration operator (RO) provides 3GPP connectivity for communication devices to request downloading and provisioning of MCIM credentials from provisioning servers. Each communication device is pre-allocated (pre-installed) a unique subscription identity such as IMSI (International Mobile Subscriber Identity) and a corresponding credential such as a secret key (hereinafter also referred to as "key" or "K") and uses the subscription identity and key to attach to the RO. To pre-allocate a unique pair of IMSI/K to each communication device for initial connectivity has the following drawbacks. First, it takes cost that the RO delivers unique pairs of IMSI/K to device manufactures and the device manufactures configure the unique pairs of IMSI/K to their communication devices. Second, some of the pre-allocated IMSI may not be used when the

communication device supports radio access technology other than 3GPP network access technology. This leads to waste IMSI numbering space.

[0003] A solution to overcome the above drawbacks is to pre-allocate the single same pair of IMSI/K to a plurality of communication devices. However, this solution also has drawbacks. Because the RO cannot handle a plurality of attachment requests with the same IMSI at the same time, it is required to carefully manage when and which communication devices can use the common IMSI to attach to the RO for the MCIM provisioning. This is, however, obviously cumbersome and costly because careful scheduling is needed and careful modification of the schedule needs to be performed when another communication device is added with the common IMSI.

SUMMARY

[0004] The present invention is intended to address the above-described problem, and it is a feature thereof to introduce a technology for allocating a unique subscription identity to a communication device having a common subscription identity.

[0005] According to an aspect of the present invention, there is provided an authentication server. The server includes a receiving unit configured to

receive an authentication data request from a network apparatus. The authentication data request includes a subscription identity. The server further includes a determination unit configured to determine whether the received subscription identity is a predetermined subscription identity and an obtaining unit configured to obtain, when it is determined that the received subscription identity is the predetermined subscription identity, a key and a subscription identity other than the received subscription identity. The key is derived by applying a key derivation function to a random number and a key associated with the predetermined subscription identity. The server further includes a storage unit configured to store the obtained key and the obtained subscription identity such that the obtained key is associated with the obtained subscription identity and a response unit configured to send an authentication data response including the random number and an authentication token to the network apparatus. The authentication token includes the obtained subscription identity.

[0006] According to another aspect of the present invention, there is provided a communication device. The device includes a sending unit configured to send an attach request to a network apparatus. The attach request includes a subscription identity. The device further includes a receiving unit configured to receive

an authentication request from the network apparatus as a response of the attach request. The authentication request includes a random number and an authentication token. The device further includes an obtaining unit configured to obtain a key and a subscription identity. The subscription identity is obtained from the received authentication request and the key is derived by applying a key derivation function to the received random number and a key associated with the sent subscription identity. The device further includes a storage unit configured to store the obtained key and the obtained subscription identity such that the obtained key is associated with the obtained subscription identity and a response unit configured to send an authentication failure to the network apparatus.

[0007] Further features of the present invention will become apparent from the following description of exemplary embodiments with reference to the attached drawings, in which like reference characters designate the same or similar parts throughout the figures thereof.

BRIEF DESCRIPTION OF DRAWINGS

[0008] Fig. 1 illustrates an exemplary overall system 100 according to some embodiments of the present invention.

[0009] Fig. 2 illustrates an exemplary block

diagram of the authentication server according to some embodiments of the present invention.

[0010] Fig. 3 illustrates an exemplary block diagram of the communication device according to some embodiments of the present invention.

[0011] Fig. 4 illustrates exemplary operations of the system in Fig. 1 according to some embodiments of the present invention

DETAILED DESCRIPTION

[0012] Embodiments of the present invention will now be described with reference to the attached drawings. Each embodiment described below will be helpful in understanding a variety of concepts from the generic to the more specific. It should be noted that the technical scope of the present invention is defined by claims, and is not limited by each embodiment described below. In addition, not all combinations of the features described in the embodiments are always indispensable for the present invention.

[0013] Fig. 1 illustrates an exemplary overall system 100 according to some embodiments of the present invention. The system 100 may include a communication device 110 and networks 120 and 130. The system 100 may include more than one communication device and the communication device 110 represents any one of the communication devices included in the system 100. The

following description uses an IMSI and secret key as a subscription identity and credential. However, the present invention can apply to any type of subscription identities and credentials which are used in attachment procedures.

[0014] The network 120 is a network managed by a visited network operator (VNO) and includes a network apparatus 121. The network 120 may be also referred to as a VNO network 120. The network apparatus 121 provides temporary 3GPP network access to the communication device 110. The network apparatus 121 may provide full or restricted connectivity during initial access. The network apparatus 121 may be implemented in a Visitor Location Register (VLR) or a Serving GPRS Support Node (SGSN) of the VNO network 120.

[0015] The network 130 is a network managed by a registration operator (RO) and includes an authentication server 131. The network 130 may be also referred to as an RO network 130. The authentication server 131 provides initial connectivity to the communication device 110 and provides registration and provisioning functions for the communication device 110. The authentication sever 131 may be implemented in a Home Location Register (HLR) of the RO network 130.

[0016] The communication device 110 is a device which can attach to the RO network 130 by use of a pair of IMSI/K. Examples of the communication device 110

include a mobile phone, a personal computer, a navigation device in a vehicle, a security camera, and so on.

[0017] The system 100 may include a network (not shown) managed by a selected home operator (SHO) which is a network operator with capability of providing network connectivity to the communication device 110, as described in 3GPP TR 33.812.

[0018] Fig. 2 illustrates an exemplary block diagram of the authentication server 131. The authentication server 131 may comprise a CPU 201, a memory 202, a receiving unit 203, a determination unit 204, an obtaining unit 205, a response unit 206, a random number generator 207, and a storage device 208.

[0019] The CPU 201 controls overall operations of the authentication server 131. The memory 202 stores computer programs and data used in operations of the authentication server 131. The random number generator 207 generates random numbers. The storage device 208 is typically implemented by a nonvolatile storage device such as a hard disk drive and stores a special IMSI list 209 and a mapping table 210. Functions of the receiving unit 203, the determination unit 204, the obtaining unit 205, and the response unit 206 will be described in detail later with reference to Fig. 4. These functions may be implemented in form of computer programs to be executed by the CPU 201.

[0020] The special IMSI list 209 stores special IMSIs. As used herein, the special IMSI means an IMSI which is shared among a plurality of communication devices. On the other hand, as used herein, a normal IMSI means an IMSI which is uniquely allocated to a communication device and used in authentication procedure (that is, AKA procedure) or attachment procedure between a communication device and the authentication server 131. The authentication server 131 regards an IMSI included in the special IMSI list 209 as a special IMSI and an IMSI not included in the special IMSI list 209 as a normal IMSI. The RO may add to the special IMSI list 209 an IMSI which was provided to, for example, device manufactures so as to be shared among communication devices of the manufactures. The mapping table 210 stores pairs of IMSI and key. In the mapping table 210, each IMSI is associated with a corresponding key. The mapping table 210 includes entries for special IMSIs and normal IMSIs.

[0021] Fig. 3 illustrates an exemplary block diagram of the communication device 110. The communication device 110 may comprise a CPU 301, a memory 302, a use interface 303, a network interface 304, a sending unit 305, a receiving unit 306, an obtaining unit 307, a response unit 308, a trusted environment (TRE) 309, and an authentication unit 310.

[0022] The CPU 301 controls overall operations of

the communication device 110. The memory 302 stores computer programs and data used in operations of the communication device 110. The user interface 303 provides an interface with a human such as the user of the communication device 110 and includes a display, a keypad, a speaker, and the like, for example. The network interface 304 provides an interface with other devices such as the network apparatus 121, the authentication server 131, and the likes. Functions of the sending unit 305, the receiving unit 306, the obtaining unit 307, the response unit 308, and an authentication unit 310 will be described in detail later with reference to Fig. 4. These functions may be implemented in form of computer programs to be executed by the CPU 301.

[0023] The TRE 309 provides some hardware and software protection and separation for the provisioning, storage, execution, and management of subscription modules. The TRE 309 may have a pre-installed subscription module. In some embodiments of the present invention, the TRE 309 stores a special IMSI (hereinafter referred to as "IMSI0") and a corresponding key (hereinafter referred to as "K0"). IMSI0 and K0 may be pre-installed during the manufacture of the communication device 110. Alternatively, IMSI0 and K0 may be included in a memory card which a user of the communication device 110

inserts to the communication device 110. Generally speaking, IMSI0 and K0 may be stored in the communication device 110 in a secure way.

[0024] Fig. 4 illustrates exemplary operations of the system 100 according to some embodiments of the present invention. The CPUs included in the communication device 110, a network apparatus 121, and the authentication server 131 may execute computer programs stored in their memories to process these operations. It is assumed that both of the communication device 110 and the authentication server 131 stores a special IMSI (IMSI0) and a corresponding key (K0) before the following operations are performed.

[0025] In step S1, the sending unit 305 of the communication device 110 sends an attach request to the network apparatus 121 in order to obtain a normal IMSI (that is, a unique IMSI). The attach request to be sent includes IMSI0. The network apparatus 121 receives this attach request. Although this attach request includes a special IMSI, this attach request can take the same format as an attach request used in a normal attachment procedure so that the network apparatus 121 can handle this attach request in the same way as the normal attachment procedure. As used herein, the normal attachment procedure means an attachment procedure using a normal IMSI, such as defined in 3GPP TS 33.102 for example.

[0026] In step S2, the network apparatus 121 sends an authentication data request to the authentication server 131 in order to obtain a random number (hereinafter referred to as "RAND") and an authentication token (hereinafter referred to as "AUTN"). The authentication data request to be sent includes IMSI0 extracted from the received attach request. The receiving unit 203 of the authentication server 131 receives this authentication data request. This authentication data request can take the same format as an authentication data request used in the normal attachment procedure.

[0027] In step S3, the determination unit 204 of the authentication server 131 determines whether an IMSI extracted from the received authentication data request (that is, IMSI0) is a special IMSI or a normal IMSI, for example by determining whether the extracted IMSI is included in the special IMSI list 209. When it is determined that the extracted IMSI is a normal IMSI, the authentication server 131 performs the normal attachment procedure. Details for the normal attachment procedure are omitted because it is well known to those skilled in the art.

[0028] When it is determined that the extracted IMSI is a special IMSI, the procedure goes to step S4. In step S4, the obtaining unit 205 of the authentication server 131 obtains a new normal (unique)

IMSI (hereinafter referred to as "IMSI1") and a new corresponding key (hereinafter referred to as "K1"). The obtaining unit 205 may obtain IMSI1 by generating a new unique IMSI or by requesting another server to generate a new unique IMSI. The obtaining unit 205 may obtain K1 by applying a key derivation function (KDF) to a RAND and the key (that is, K0) associated with IMSI0. That is, K1 is derived from the equation K1 = KDF(K0, RAND). Any type of standard key derivation functions may be used of the KDF in step S4. The obtaining unit 205 may obtain the RAND using the random number generator 207. The obtaining unit 205 may obtain the key associated with IMSI0 by referring to the mapping table 210.

[0029] In step S5, the obtaining unit 205 stores the obtained IMSI1 and K1 in the mapping table 210 such that K1 is associated with the IMSI1 for future use.

[0030] In step S6, the response unit 308 of the authentication server 131 sends an authentication data response to the network apparatus 121 in order to respond to the authentication data request received in step S2. The authentication data response to be sent includes the RAND obtained in step S4 and an AUTN including the IMSI obtained in step S4 (that is, IMSI1). The network apparatus 121 receives this authentication data response. An example of AUTN encoding, an IMSI consists of 15 digits, which are smaller than 60 bits,

and an AUTN is 128 bits. Therefore, an AUTN can carry all bits of an IMSI. The AUTN may include the IMSI in the first 60 bits and the remaining bits of the AUTN may be filled with 1 for example. The AUTN may include IMSI1 in the last 60 bits instead of the first 60 bits. Generally speaking, the AUTN may be derived by applying any suitable function to IMSI1 such that the communication device 110 can obtain IMSI1 by applying a reverse function to the AUTN.

[0031] This authentication data response can take the same format as an authentication data response used in a normal attachment procedure. According to the normal attachment procedure, an authentication data response also includes a ciphering key (CK), an integrity key (IK), and an expected response (XRES). In order to comply with the format of the authentication data response used in the normal attachment procedure, the response unit 308 fills CK, IK, and XRES in the authentication data response to be sent in step S6 with arbitrary values.

[0032] In step S7, the network apparatus 121 sends an authentication request to the communication device 110 in order to authenticate the communication device 110. The authentication data request to be sent includes the RAND and AUTN extracted from the received authentication data response. The receiving unit 306 of the communication device 110 receives this

authentication request.

[0033] In step S8, the authentication unit 210 may authenticate the AUTN included in the received authentication request, using the RAND included in this request and K0. This authentication will fail because the AUTN was not generated according to the normal attachment procedure. This step may be skipped because the sending unit 305 sent the attach request including a special IMSI in step S1 and thus the authentication unit 210 can forecast that the authentication will fail. In some embodiment, the procedure goes to step S9 after it is determined that the authentication in step S8 fails.

[0034] In step S9, the response unit 308 of the communication device 110 sends an authentication failure message to the network apparatus 121 to inform that authentication of the AUTN fails. As described above, the authentication of the AUTN may or may not be actually performed. Failure code in the authentication failure message may be "MAC failure" or "GSM authentication unacceptable" described in 3GPP TS 24.008. The network apparatus 121 receives this authentication failure message.

[0035] In step S10, the network apparatus 121 sends an authentication failure report to the authentication server 131 to inform that the authentication of the AUTN fails in the communication

device 110. The authentication server 131 may confirm that IMSI1 has been successfully delivered to the communication device 110 based on receiving of the authentication failure report.

[0036] In step S11, the obtaining unit 307 of the communication device 110 obtains IMSI1 and a key. The obtaining unit 307 may obtain IMSI1 by extracting IMSI1 from the AUTN which was received in step S7. The obtaining unit 307 may apply to the ATUN the inverse function of the function which was used in step S6 in order to obtain the AUTN from IMSI1. In this case, the reverse function may be stored in the communication device 110 (for example, in the TRE 309) before the procedure shown in Fig. 4 begins. In some embodiments, the reverse function may be allocated to the communication device 110 when IMSI0 and K0 are allocated to the communication device 110.

[0037] The obtaining unit 307 may obtain a key by applying the KDF to the RAND included in the authentication request in step S7 and K0 stored in the TRE 309, that is, by calculating KDF(K0, RAND). The KDF used in step S11 is the same function as the KDF used in step S4. Thus, the obtained key is equal to K1 because the arguments applied to the KDF are the same in steps S4 and S11. The KDF may be stored in the communication device 110 (for example, in the TRE 309) before the procedure shown in Fig. 4 begins. In some

embodiments, the KDF may be allocated to the communication device 110 when IMSI0 and K0 are allocated to the communication device 110.

[0038] In step S12, the obtaining unit 307 stores IMSI1 and K1 in the TRE 309 such that K1 is associated with IMSI1 for future use.

[0039] After step S12, the communication device 110 can use a unique IMSI (that is, IMSI1) and a corresponding key (that is, K1) which the authentication server 131 also stores. The communication device 110 therefore can perform the normal attachment procedure using IMSI1 and K1. In one embodiment, in step S13, the sending unit 305 of the communication device 110 sends another attach request including IMSI1 to the network apparatus 121 to attach to the RO network 130. In step S14, the network apparatus 121 sends to an authentication data request including IMSI1 to the authentication server 131. The remaining operations will be understood by those skilled in the art and their descriptions omitted.

[0040] In another embodiment, the network apparatus 121 may send an identity request to the communication device 110 after receiving the authentication failure message in step S9. The communication device 110 sends an identity response including IMSI1. Descriptions of the remaining operations are omitted because they are specified in

the 3GPP TS24.008.

[0041] In order to reduce a risk of DoS (Denial of Service) attack for a special IMSI, the authentication server 131 may set rate limit for authentication data requests from the network apparatus 121, shorter valid period for allocated IMSI1, or the like.

[0042] According to the embodiments of the present invention, a single same pair of subscription identity and secret key is shared among a plurality of communication devices and a unique pair of subscription identity and secret key is allocated to a communication device on demand. This avoids wasting a numbering space of subscription identities. Moreover, the cost to coordinate for collision avoidance in terms of initial connectivity establishment can be removed.

[0043] The communication device and the authentication server can share a secret key associated with the delivered subscription identity in a secure way because this secret key is not communicated via networks.

[0044] During the procedure for delivering a unique subscription identity, the network apparatus relaying communication between the communication device and the authentication server can handle messages in the same way as in the normal attachment procedure. Thus, the present invention is applicable to the scenario where the communication device is located in a

visited network, without changing configuration of the network apparatus such as a VLR and SGSN.

[0045] While the present invention has been described with reference to exemplary embodiments, it is to be understood that the invention is not limited to the disclosed exemplary embodiments. The scope of the following claims is to be accorded the broadest interpretation so as to encompass all such modifications and equivalent structures and functions.

CLAIMS

1. An authentication server (131) comprising:

a receiving unit (203) configured to receive an authentication data request from a network apparatus (121), wherein the authentication data request includes a subscription identity,

a determination unit (204) configured to determine whether the received subscription identity is a predetermined subscription identity;

an obtaining unit (205) configured to obtain, when it is determined that the received subscription identity is the predetermined subscription identity, a key and a subscription identity other than the received subscription identity, wherein the key is derived by applying a key derivation function to a random number and a key associated with the predetermined subscription identity;

a storage unit (208) configured to store the obtained key and the obtained subscription identity such that the obtained key is associated with the obtained subscription identity; and

a response unit (206) configured to send an authentication data response including the random number and an authentication token to the network apparatus, wherein the authentication token includes the obtained subscription identity.

2. The server according to claim 1, wherein the subscription identity obtained by the obtaining unit is a unique subscription identity.

3. A communication device (110) comprising:

a sending unit (305) configured to send an attach request to a network apparatus (120), wherein the attach request includes a subscription identity;

a receiving unit (306) configured to receive an authentication request from the network apparatus as a response of the attach request, wherein the authentication request includes a random number and an authentication token;

an obtaining unit (307) configured to obtain a key and a subscription identity, wherein the subscription identity is obtained from the received authentication request and the key is derived by applying a key derivation function to the received random number and a key associated with the sent subscription identity;

a storage unit (309) configured to store the obtained key and the obtained subscription identity such that the obtained key is associated with the obtained subscription identity; and

a response unit (308) configured to send an authentication failure to the network apparatus.

4. The device according to claim 3, wherein the sending unit is further configured to send an attach request to the network apparatus after sending the authentication failure, wherein the attach request includes the obtained subscription identity.

5. The device according to claim 3 or 4, further comprising an authentication unit (310) configured to authenticate the received authentication token using the received random number and a key associated with the sent subscription identity,

wherein the obtaining unit is further configured to obtain the key and the subscription when the authentication of the received authentication token fails.

FIG. 1

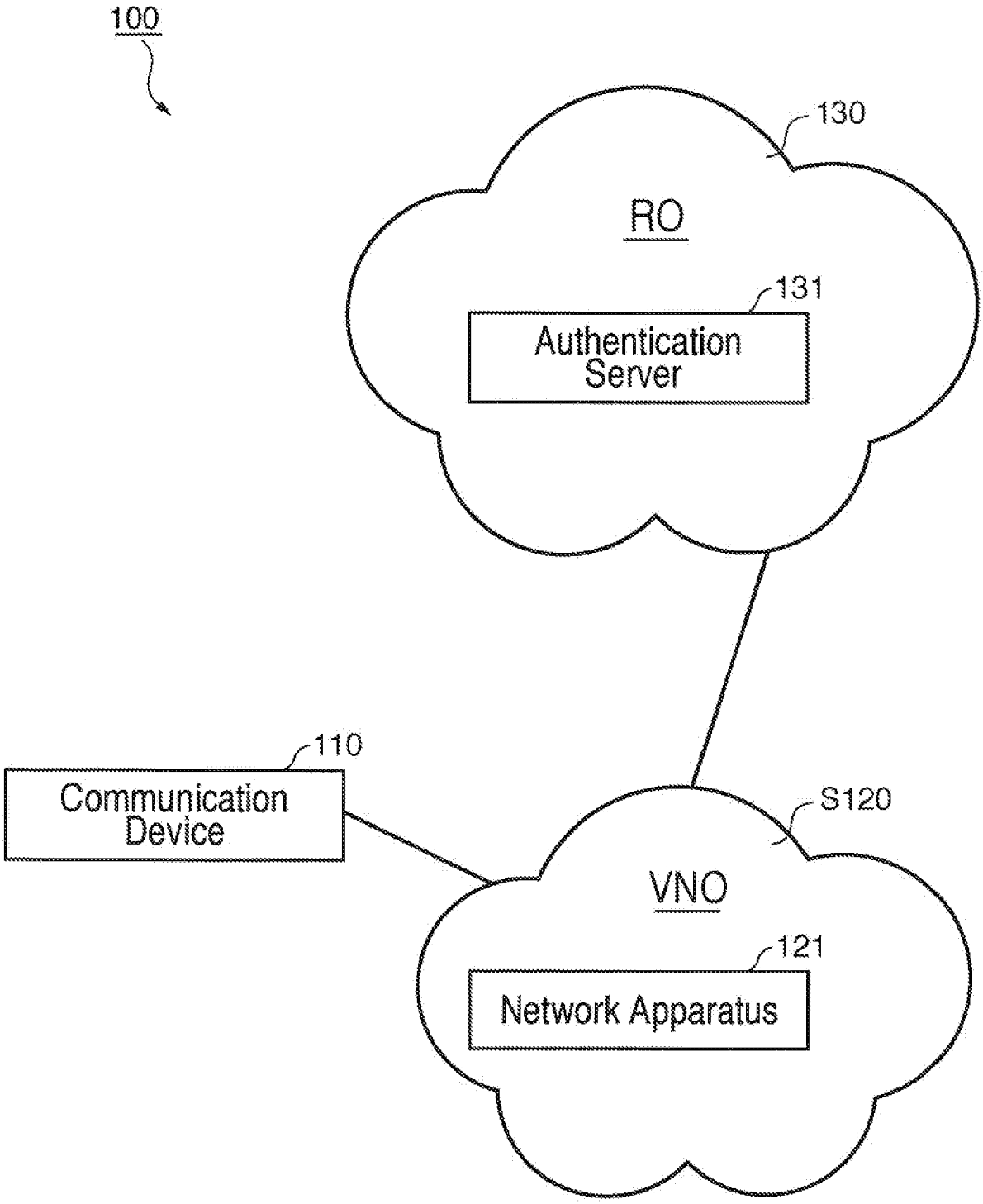

100
130
RO
131
Authentication Server
110
Communication Device
S120
VNO
121
Network Apparatus

FIG. 2

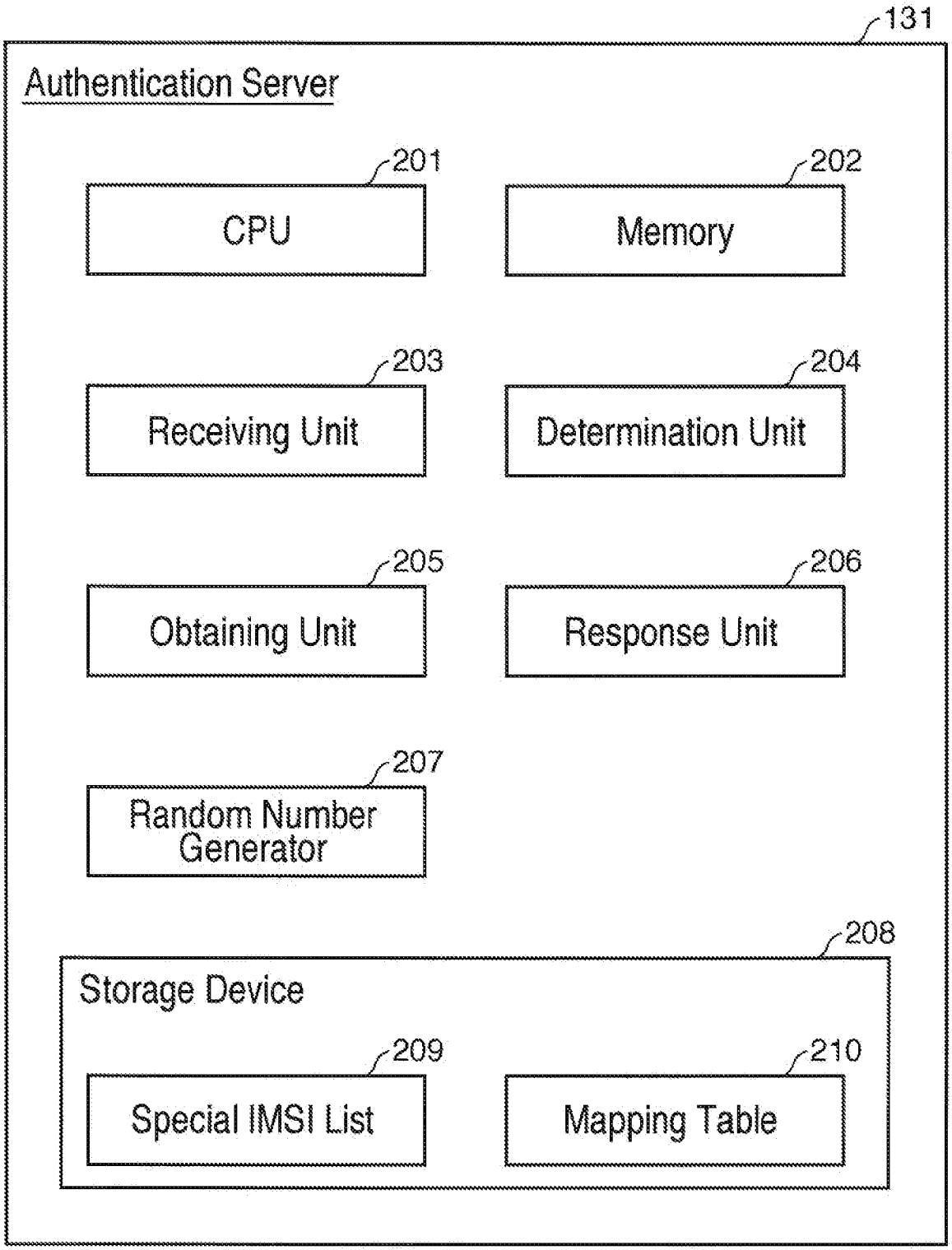

131
Authentication Server
201
CPU
202
Memory
203
Receiving Unit
204
Determination Unit
205
Obtaining Unit
206
Response Unit
207
Random Number Generator
208
Storage Device
209
Special IMSI List
210
Mapping Table

FIG. 3

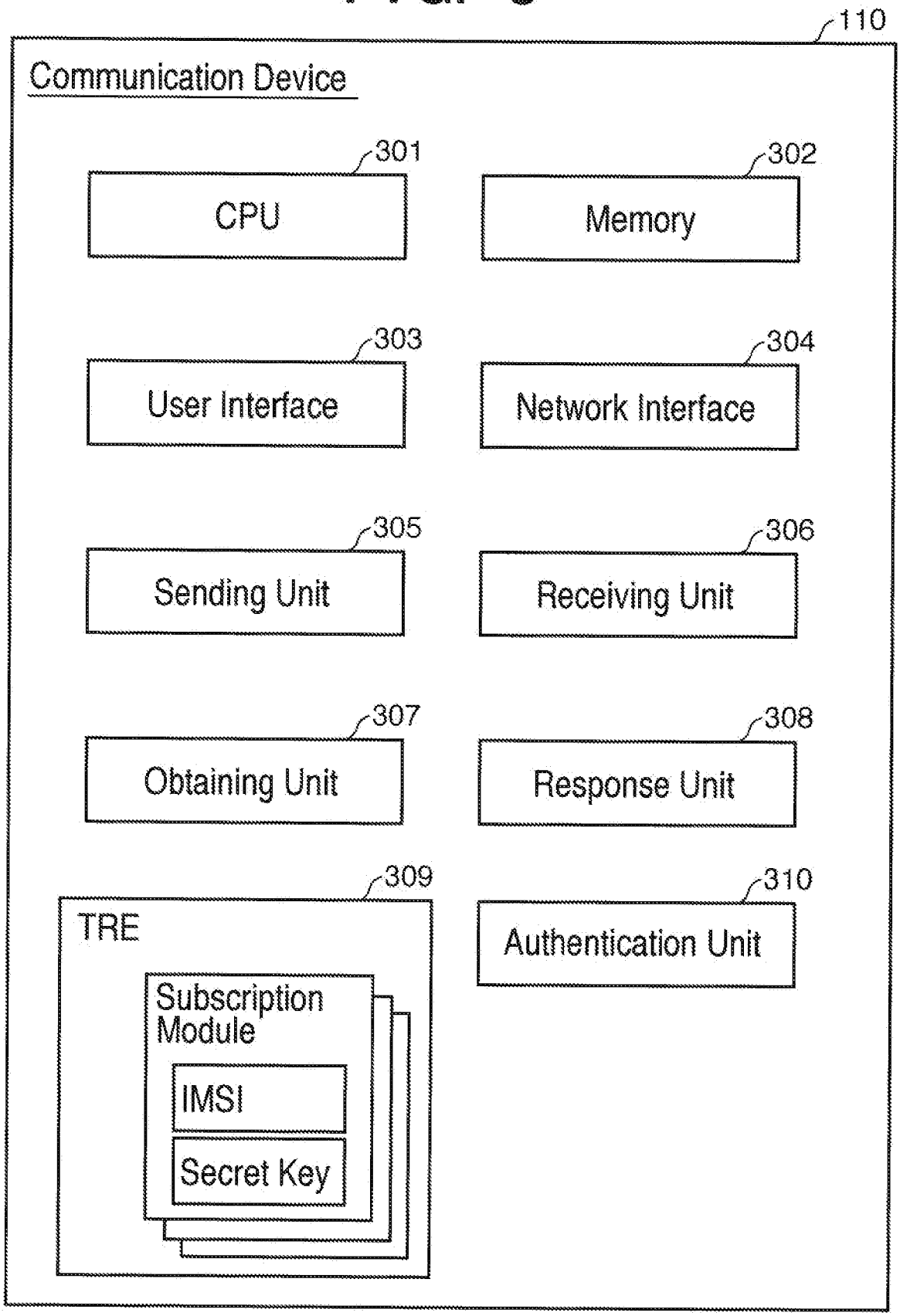
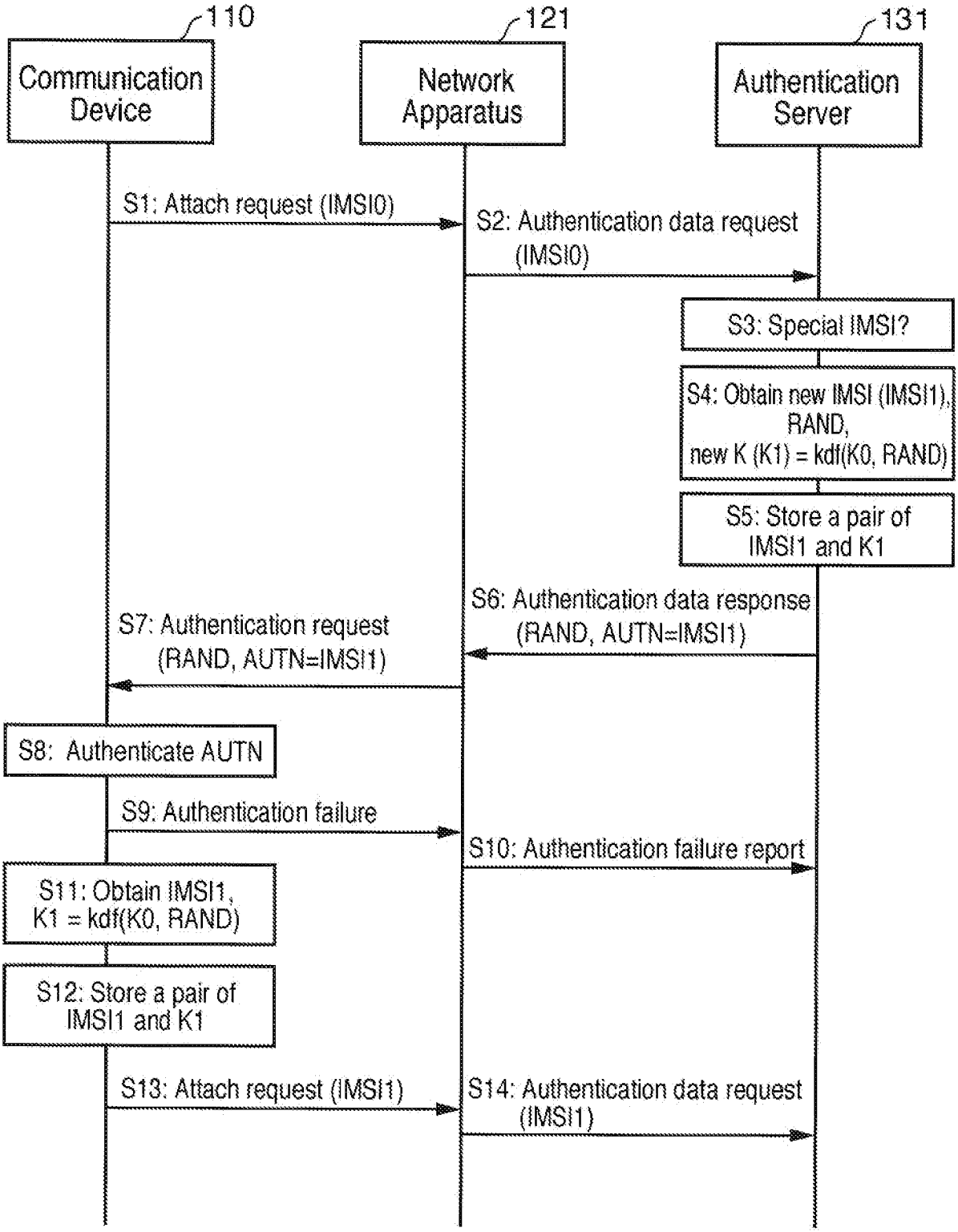

110
Communication Device
301
CPU
302
Memory
303
User Interface
304
Network Interface
305
Sending Unit
306
Receiving Unit
307
Obtaining Unit
308
Response Unit
309
TRE
Subscription Module
IMSI
Secret Key
310
Authentication Unit

FIG. 4


110
121
131
Communication Device
Network Apparatus
Authentication Server
S1: Attach request (IMSI0)
S2: Authentication data request (IMSI0)
S3: Special IMSI?
S4: Obtain new IMSI (IMSI1), RAND, new K (K1) = kdf(K0, RAND)
S5: Store a pair of IMSI1 and K1
S6: Authentication data response (RAND, AUTN=IMSI1)
S7: Authentication request (RAND, AUTN=IMSI1)
S8: Authenticate AUTN
S9: Authentication failure
S10: Authentication failure report
S11: Obtain IMSI1, K1 = kdf(K0, RAND)
S12: Store a pair of IMSI1 and K1
S13: Attach request (IMSI1)
S14: Authentication data request (IMSI1)

INTERNATIONAL SEARCH REPORT

International application No
PCT/SE2011/050759

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04W12/06 H04L29/06 H04W8/18 H04W8/20
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 practical, search terms used)
EPO-Internal, COMPENDEX, INSPEC, IBM-TDB, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 2 222 105 A1 (NTT DOCOMO INC [JP]) 25 August 2010 (2010-08-25) abstract paragraph [0005] - paragraph [0006] paragraph [0015] - paragraph [0018]; figure 1 paragraph [0084] - paragraph [0093]; figure 6 paragraph [0094] - paragraph [0105]; figure 7	1-5

A	US 2009/191918 A1 (MARDIKS EITAN [IL]) 30 July 2009 (2009-07-30) abstract paragraph [0033] - paragraph [0037] figure 3 figures 4A, 4B	1-5

	-/--	

[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 document 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
24 February 2012	01/03/2012

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	Poppe, Fabrice

INTERNATIONAL SEARCH REPORT

International application No
PCT/SE2011/050759

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 98/56201 A2 (SONERA OY [FI]; LINKOLA JANNE [FI]; BLOMBERG OLAVI [FI]) 10 December 1998 (1998-12-10) abstract page 2, line 31 - page 3, line 21 page 3, line 31 - page 4, line 12	1-5
A	"3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Feasibility study on the security aspects of remote provisioning and change of subscription for Machine to Machine (M2M) equipment (Release 9)", 3GPP STANDARD; 3GPP TR 33.812, 3RD GENERATION PARTNERSHIP PROJECT (3GPP), MOBILE COMPETENCE CENTRE ; 650, ROUTE DES LUCIOLES ; F-06921 SOPHIA-ANTIPOLIS CEDEX ; FRANCE, no. V9.2.0, 22 June 2010 (2010-06-22), pages 1-87, XP050441986, [retrieved on 2010-06-22] cited in the application the whole document	1-5
A	"3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security architecture (Release 10)", 3GPP STANDARD; 3GPP TS 33.102, 3RD GENERATION PARTNERSHIP PROJECT (3GPP), MOBILE COMPETENCE CENTRE ; 650, ROUTE DES LUCIOLES ; F-06921 SOPHIA-ANTIPOLIS CEDEX ; FRANCE, no. V10.0.0, 28 December 2010 (2010-12-28), pages 1-72, XP050462445, [retrieved on 2010-12-28] cited in the application the whole document	1-5

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/SE2011/050759

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 2222105 A1	25-08-2010	CN 101800980 A	11-08-2010
		EP 2222105 A1	25-08-2010
		JP 2010177792 A	12-08-2010
		KR 20100087662 A	05-08-2010
		US 2010190473 A1	29-07-2010
US 2009191918 A1	30-07-2009	NONE	
WO 9856201 A2	10-12-1998	AT 281742 T	15-11-2004
		AU 7657198 A	21-12-1998
		CA 2292656 A1	10-12-1998
		DE 69827385 D1	09-12-2004
		DE 69827385 T2	10-11-2005
		EE 9900559 A	15-06-2000
		EP 0986925 A2	22-03-2000
		ES 2231987 T3	16-05-2005
		FI 972369 A	05-12-1998
		IL 133158 A	01-08-2006
		NZ 501327 A	26-01-2001
		US 6934391 B1	23-08-2005
		WO 9856201 A2	10-12-1998