(19) DANMARK

(10) **DK/EP 3598690 T3**

Patent- og
Varemærkestyrelsen

(12) Oversættelse af
europæisk patentskrift

(51) Int.Cl.: ***H 04 W 12/041 (2021.01)*** ***H 04 L 9/08 (2006.01)*** ***H 04 L 29/06 (2006.01)*** ***H 04 W 8/20 (2009.01)*** ***H 04 W 12/0471 (2021.01)*** ***H 04 W 92/10 (2009.01)***

(45) Oversættelsen bekendtgjort den: **2022-01-10**

(80) Dato for Den Europæiske Patentmyndigheds
bekendtgørelse om meddelelse af patentet: **2021-12-08**

(86) Europæisk ansøgning nr.: **19183523.0**

(86) Europæisk indleveringsdag: **2008-05-20**

(87) Den europæiske ansøgnings publiceringsdag: **2020-01-22**

(30) Prioritet: **2007-09-17 US 97295507 P**

(62) Stamansøgningsnr: **13163049.3**

(84) Designerede stater: **AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MT NL NO PL PT RO SE SI SK TR**

(73) Patenthaver: **Telefonaktiebolaget LM Ericsson (publ) , 164 83 Stockholm, Sverige**

(72) Opfinder: **Blom, Rolf, Svärdvägen 2, 175 68 Järfälla, Sverige**
MILDH, Gunnar, Koltrastvägen 28, 192 55 Sollentuna, Sverige
NORRMAN, Karl, Stigbergsgatan 32A, 116 28 Stockholm, Sverige

(74) Fuldmægtig i Danmark: **Zacco Denmark A/S, Arne Jacobsens Allé 15, 2300 København S, Danmark**

(54) Benævnelse: **Fremgangsmåde og indretning i et telekommunikationssystem**

(56) Fremdragne publikationer:

3GPP: "3RD GENERATION PARTNERSHIP PROJECTS; TECHNICAL SPECIFICATION GROUP SERVICES AND SYSTEM ASPECTS; RATIONALE AND TRACK OF SECURITY DECISIONS IN LONG TERM EVOLVED (LTE) RAN/3GPP SYSTEM ARCHITECTURE EVOLUTION (SAE) (RELEASE 8)", INTERNET CITATION, 20 February 2007 (2007-02-20), XP002445696, Retrieved from the Internet: URL:http://www.3gpp1.net/ftp/spces/archive/33%5Fseries/33.821/ [retrieved on 2007-08-06]

3GPP: "3rd Generation Partnership Project;Technical Specification Group Services and System Aspects;3GPP System Architecture Evolution:Security Architecture;Release 8", 3GPP DRAFT; DRAFT S3-070624 V1 UPDATE OF 479_33ABC V000 SAE-LTE-SEC RM, 3RD GENERATION PARTNERSHIP PROJECT (3GPP), MOBILE COMPETENCE CENTRE ; 650, ROUTE DES LUCIOLES ; F-06921 SOPHIA-ANTIPOLIS CEDEX ; FRANCE, vol. SA WG3, no. Montreal; 20070712, 12 July 2007 (2007-07-12), XP050279972,

DESCRIPTION

TECHNICAL FIELD

[0001] The present invention relates to methods and devices in a telecommunication system, and in particular to a security solution in the EPS (Evolved Packet System), i.e. the E-UTRAN (the Evolved UMTS Terrestrial Radio Access Network) and the EPC (Evolved Packet Core network), for UE-triggered service requests. More specifically, the present invention relates a method and an arrangement in an MME (Mobility Management Entity) and in a UE (User Equipment) for an EPS (Evolved Packet System) of establishing a security key for protecting RRC/UP traffic.

BACKGROUND

[0002] In the EPS-architecture, the subscriber authentication is performed between a UE and an MME (Mobility Management Entity), and the MME manages e.g. the mobility, the UE-identities and the security parameters. The basis for defining the security procedure in the EPS is a security key, K_ASME, which is shared between the MME and the UE, and established at the authentication of the UE. A functional entity of the EPS-architecture called the ASME (Access Security Management Entity) may e.g. be co-located with the MME, and the ASME receives and stores the security key K_ASME derived from the CK/IK-keys confined in the home network. From the security key, K_ASME, the ASME derives an NAS security context used to protect the NAS signalling, i.e. the Non Access Stratum signalling between the MME of the Evolved Packet Core (EPC) network and a UE. The NAS security context contains parameters for the encryption and integrity protection of the NAS signalling, such as K_NAS_enc, K_NAS_int, as well as uplink and downlink sequence numbers, NAS_U_SEQ and NAS_D_SEQ, and the sequence numbers are used to prevent replay of old messages, as well as for input to the encryption and integrity protection procedures. The ASME provides the MME with the NAS security context, and one NAS security context is kept in the MME, and a corresponding NAS security context is kept in the UE, and the replay protection, integrity protection and encryption are based on that the sequence numbers of the NAS security contexts of the MME and UE are not reused.

[0003] Preferably, the security context for the protection of the UP/RRC traffic between a UE and the serving eNodeB (i.e. a radio base station in an EPS-architecture) is also based on said security key, K_ASME. The procedure to establish the UP/RRC security context involves deriving a key called K_eNB, from which the encryption key K_eNB_UP_enc is derived for protecting the UP (User Plane), i.e. the end user data transferred over EPC and E-UTRAN, as well as the encryption key, K_eNB_RRC_enc, and the integrity protection key, K_eNB_RRC_int, for protecting the RRC (Radio Resource Control).

[0004] Figure 1 illustrates a conventional exemplary signalling flow for a UE-initiated IDLE to ACTIVE state transition in an EPS-architecture. An IDLE UE is only known to the EPC (Evolved Packet Core) of the EPS, and no UP/RRC security context exists between the eNodeB and the UE. An UE in the ACTIVE state is known both in the EPC and in the EUTRAN, and a UP/RRC security context has been established for protection of the UP/RRC-traffic between the UE and its serving eNobeB.

[0005] Figure 1 illustrates a UE 11, an eNodeB 12, an MME 13, a serving GW (Gateway) 14, a PDN Gateway 15, and the HSS (Home Subscriber Server) 16. The Serving Gateway 14 is the node of the EPC that terminates the interface towards EUTRAN, and the PDN Gateway is the node of the EPC that terminates the interface towards a PDN (Packet Data Network). If a UE accesses multiple PDNs, there may be multiple PDN Gateways for that UE. In signal S1 and signal S2, the NAS Service Request is transparently forwarded from the UE to the MME, and the NAS Service Request is integrity protected based on NAS_U_SEQ. In the optional signal S3, the UE is authenticated by the MME and the K_ASME is established, using subscriber data stored in the HSS (Home Subscriber Server), and the MME sends the Initial Context Setup Request to the eNodeB, in S4. In the signals S5 and S6, the eNodeB establishes the radio bearer with the UE and forwards uplink data, and returns an Initial Context Setup Complete-message to the MME in signal S7. In signal S8, the MME sends an update bearer request to the Serving GW, and the serving GW responds in signal S9.

[0006] In prior solutions, the derivation of the K_eNB by the UE and MME for the RRC/UP security context is based e.g. on a NAS SERVICE ACCEPT message or other explicit information sent from the MME to the UE. However, as illustrated in the exemplary conventional EPS signalling flow in figure 1, the MME will normally not send any NAS SERVICE ACCEPT upon receiving a NAS SERVICE REQUEST from a UE in an EPS. Therefore, it will not be possible to derive the K_eNB from the information in a NAS SERVICE ACCEPT message.

[0007] According to an exemplary known solution, the K_eNB is derived by the MME from the K_ASME and the NAS_D_SEQ used by the MME in the NAS SERVICE ACCEPT message, and the UE derives the same K_eNB by retrieving the sequence number, NAS_D_SEQ, from the NAS SERVICE ACCEPT message and performing the same K_eNB derivation as the MME. The MME transfers the K_eNB to the eNodeB when it sets up the S1-connenction to the eNodeB. However, a drawback with this known solution is that if no explicit NAS SERVICE ACCEPT message is defined from the MME to the UE, as in the exemplary conventional EPS signalling flow in figure 1, it is not possible for the UE to derive the same K_eNB as the MME. Even though it is technically possible for the UE to estimate a current NAS downlink sequence number, NAS_D_SEQ, this estimation could be erroneous, since the MME may have sent NAS messages that were lost and never received by the UE. In such a case, the MME would have updated its NAS_D_SEQ, without the UE being aware of the updating, leading to an erroneous NAS_D_SEQ in the UE.

[0008] According to another exemplary known solution, the derivation of the K_eNB is based on a separate sequence number maintained specifically for the derivation of the K_eNB, and this sequence number is explicitly synchronized during the NAS Service Request procedure either by the UE sending it to the MME, or by the MME sending it to the UE. However, a drawback with this solution is the extra complexity of the separate sequence number, since it has to be maintained both in the UE and in the MME in order to prevent replay attacks.

SUMMARY

[0009] The object of the present invention is to address the problem outlined above, and this object and others are achieved by the method and arrangement according to the independent claims, and by the embodiments according to the dependent claims

[0010] The basic idea of the present invention is that the K_eNB is derived from the K_ASME and from the NAS_U_SEQ of the NAS SERVICE REQUEST message from the UE to the MME, thereby triggering the establishment of a UP/RRC security context in the eNodeB.

[0011] It is an advantage of the present invention that no explicit downlink NAS SERVICE ACCEPT message or sequence number from the MME to the UE is required, and that the replay protection functionality of the NAS security context is re-used in the RRC and UP security contexts.

[0012] The invention is defined by the independent claims. Further embodiments are defined by the dependent claims.

BRIEF DESCRIPTION OF THE DRAWINGS

[0013] The present invention will now be described in more detail, and with reference to the accompanying drawings, in which:

- Figure 1 is signalling diagram illustrating a conventional UE triggered Service Request in an EPS;
- Figure 2 is a signalling diagram illustrating the first embodiment of this invention, according to which the UE remembers the NAS_U_SEQ sent to the MME in an NAS SERVICE REQUEST-message;
- Figure 3 is a flow diagram illustrating the derivation of the K_eNB by the UE and the MME;
- Figure 4 is a signalling diagram illustrating a second embodiment of this invention, in which the MME returns the received NAS_U_SEQ to the UE;
- Figure 5 is a flow diagram illustrating the second realisation depicted in the figure 4; and
- Figure 6a illustrates schematically an MME (Mobility Management Entity), and the figure 6b illustrates schematically a UE, both provided with means for deriving the security key K_eNB.

DETAILED DESCRIPTION

[0014] In the following description, specific details are set forth, such as a particular architecture and sequences of steps in order to provide a thorough understanding of the present invention. The present invention is defined by the appended claims.

[0015] Moreover, it is apparent that the described functions may be implemented using software functioning in conjunction with a programmed microprocessor or a general purpose computer, and/or using an application-specific integrated circuit. Where the invention is described in the form of a method, the invention may also be embodied in a computer program product, as well as in a system comprising a computer processor and a memory, wherein the memory is encoded with one or more programs that may perform the described functions.

[0016] The concept or the invention is that the security key, K_eNB, is derived from the Access Security Management Entity-key, K_ASME, and from the uplink sequence counter, NAS_U_SEQ, of the NAS SERVICE REQUEST message sent from the UE to the MME, thereby triggering the establishment of the UP/RRC security context in the eNodeB.

[0017] When the UE is in IDLE mode, a NAS security context exists and comprises e.g. the above described K_NAS_enc, K_NAS_int, NAS_U_SEQ and NAS_D_SEQ, and the NAS messages are integrity- and possibly confidentiality protected. The NAS security context thus also contains the security capabilities of the UE, in particular the encryption and integrity algorithms.

[0018] The protection of the NAS messages is based on the NAS security keys, K_NAS_enc, K_NAS_int, and the uplink and downlink sequence counters, NAS_U_SEQ or NAS_D_SEQ, for the direction of the message. The full sequence counter is normally not transmitted with the NAS message, only some of the low order bits, and the full sequence number will be reconstructed at the receiving end from a local estimate of the high order bits and the received low order bits.

[0019] The concept of the invention may be explained in the context of the signalling diagram for UE-triggered service requests, as depicted in the above-described figure 1:
In S1 and S2 of the conventional signalling diagram in figure 1, a NAS SERVICE REQUEST, comprising an uplink sequence counter, NAS_U_SEQ, is forwarded from the UE to the MME, and the NAS SERVICE REQUEST-message is integrity protected based on said NAS_U_SEQ. The MME checks the integrity of the message and accepts it if it is not a replay, and this guarantees that the NAS_U_SEQ is fresh and has not been used before.

[0020] Thereafter, according to this invention, the MME derives the K_eNB based at least on the received uplink sequence counter NAS_U_SEQ and on the K_ASME, using a conventional key derivation function, and this is not included in the conventional signalling diagram illustrated en figure 1. Consequently, the sequence counter may only be reset at the authentication. The MME will send the derived K_eNB down to the eNodeB in, or piggybacked to, the message of the signal S4, the Initial Context Setup Request (S1-AP).

[0021] In signal S5, the eNodeB sends a Radio Bearer Establishment and a security configuration message (Security Mode Command) to the UE. These messages may be sent as two separate messages or combined in one message, as in figure 1, and the reception of these messages by the UE will implicitly be a confirmation of the UEs NAS SERVICE REQUEST, in signal S1. The Security Mode Command will determine e.g. when the protection should start and which algorithm to use. According to this invention, the UE derives the K_eNB based at least on the NAS_U_SEQ and the K _ASME, using a conventional key derivation function, upon reception of the message in signal S5, if not performed before. Thereafter, the eNodeB and the UE will establish the UP/RRC security contexts, and this is not illustrated in the conventional signalling diagram in figure 1.

[0022] According to a first realisation, the UE stores the uplink sequence counter, NAS_U_SEQ, included in the initial NAS SERVICE REQUEST in signal S1, and uses the stored NAS_U_SEQ for the derivation of the K_eNB.

[0023] However, according to a second realisation, the MME includes the uplink sequence counter, NAS_U_SEQ, or only low order bits indicating the NAS_U_SEQ, in the S1-AP set-up message, in signal S4, sent to the eNodeB, in which case this information is also forwarded to the UE from the eNodeB during the RRC/UP context establishment. In this case, the UE will be able to retrieve the indication of the NAS _U_SEQ from the eNodeB for the derivation of the K_eNB, and does not have to keep the NAS_U_SEQ of the NAS NAS SERVICE REQUEST-message sent to the MME in the signals S1 and S2.

[0024] Figure 2 illustrates the first realisation, in which the UE keeps the NAS_U_SEQ of the initial NAS SERVICE REQUEST-message, in the signal S21, for the derivation of K_eNB in the signal S24. The MME will receive the NAS_U_SEQ from the UE in the signal S21, or only low order bits indicating the NAS_U_SEQ, and derive the K_eNB based on the NAS_U_SEQ and the K_ASME in S22. The MME forwards the derived K_eNB to the eNodeB in the signal S23.

[0025] Thereafter, not illustrated in figure 2, the eNodeB and the UE will establish the UP/RRC security context using the K_eNB, the UP/RRC security contexts comprising the encryption key, K_eNB_UP_enc for protecting the UP-traffic, as well as the encryption key and the integrity protection key, K_eNB_RRC_enc and K_eNB_RRC_int, respectively, for protecting the RRC-traffic, thereby enabling a secure UP/RRC traffic, in signal S25.

[0026] The derivation of the K_eNB is performed by a conventional key derivation function, e.g. by a Pseudo-Random Function; K_eNB = PRF(K_ASME, NAS_U_SEQ, ...).

[0027] Further, as illustrated by the dots in the above-described PRF-function, the K _eNB-deriving function may have additional conventional input values, such as e.g. the eNodeB-identity.

[0028] Figure 3 is a flow diagram illustrating the method according to this invention, and in step 31, the UE 11 sends the initial NAS SERVICE REQUEST-message to the MME 13, the message indicating the NAS uplink sequence counter, NAS_U_SEQ, normally only by sending the low order bits of the counter. In step 32, the MME receives the NAS SERVICE REQUEST-message from the UE, obtaining the NAS_U_SEQ, and reconstructing the full sequence from the received low order bits. In step 33, the MME derives the security key, K_eNB, from at least the received NAS_U_SEQ and the K_ASME from the ASME (Access Security Mobility Entity), using a suitable key derivation function, e.g. a Pseudo-Random Function.

[0029] Thereafter, the MME forwards the derived K_eNB to the eNodeB 12, in step 34, to be used by the eNodeB to establish the complete UP/RRC security context shared with the UE. In step 35, said UE will derive the same K_eNB from at least the stored K_ASME and from the NAS_U_SEQ of the initial NAS SERVICE REQUEST-message transmitted from the UE to the MME in step 31, and establish the UP/RRC security context from the derived K_eNB.

[0030] In the first realisation, the UE stores the NAS_U_SEQ transmitted to the MME in the initial NAS NAS SERVICE REQUEST-message, and uses the stored sequence number to derive the K_eNB.

[0031] Figure 4 is a signalling diagram illustrating a second realisation, in which the UE does not have to store the NAS_U_SEQ. Instead, the MME will return an indication of the received NAS_U_SEQ back to the UE, via the eNodeB. In signal S41, corresponding to the signal S21 in figure 2, the UE 11 transmits an initial NAS SERVICE REQUEST to the MME 13, indicating an uplink sequence number, NAS_U_SEQ, and MME will receive the NAS_U_SEQ and derive the K_eNB based on at least the NAS_U_SEQ and the K_ASME, in S42. However, according to this second embodiment, the MME will include an indication of said received NAS_U_SEQ in signal S43 transmitted to the eNodeB 12 together with the derived K_eNB, and the eNodeB will forward the NAS_U_SEQ to the UE, in signal S44. Thereafter, the UE will derive the K_eNB from at least the K_ASME and from the NAS_U_SEQ returned by the MME, in signal S45. From the derived security key, K_eNB, the eNodeB and the UE will establish the UP/RRC security context, thereby enabling secure UP/RRC traffic, in signal S46.

[0032] Figure 5 is a flow diagram illustrating the above-described method according to a second realisation, in which an indication of the NAS_U_SEQ is returned to the UE by the MME. In step 41, the UE 11 sends the initial NAS SERVICE REQUEST-message to the MME 13, the message indicating the NAS uplink sequence counter, NAS_U_SEQ, normally the low order bits. In step 52, the MME receives the NAS SERVICE REQUEST-message from the UE, thereby obtaining the NAS_U_SEQ, and, if necessary, reconstructing the full NAS_U_SEQ from the received low order bits. In step 53, the MME derives the security key, K_eNB, from at least the received NAS_U_SEQ and the K_ASME, using a suitable key derivation function.

[0033] Thereafter, the MME includes an indication of the NAS uplink sequence counter, NAS_U_SEQ, in the message forwarding the derived K_eNB to the eNodeB 12, in step 54, and the eNodeB uses the received security key, K eNB, for establishing a UP/RRC security context. The received NAS_U_SEQ is forwarded to the UE 11 by the eNodeB, in step 55, and in step 56, the UE derives the security key, K_eNB, from at least the K_ASME and from said received NAS_U_SEQ, in order to establish the UP/RRC security context shared with the eNodeB.

[0034] The derivation of the K_eNB by the MME, in the step 53, and by the UE, in the step 56, is performed by a suitable conventional key derivation function, e.g. a Pseudo-Random Function; K_eNB = PRF(K_ASME, NAS_U_SEQ, ,...). Normally, the key derivation function will have additional conventional input values, e.g. the eNodeB-identity.

[0035] Figure 6a illustrates an MME 13 (Mobility Management Entity) for an EPS, according to this invention, further arranged to establish a security key, K_eNB, for a security context for the protection of UP/RRC traffic between a UE and a serving eNodeB. The MME is provided with conventional communication means, not illustrated in the figure, for communicating with the nodes in the EPS, e.g. with the eNodeBs via an S1-MME interface. Further, in the MME of figure 1, an ASME (Access Security Management Entity) 61 is illustrated by hatched lines, since this functional entity of an EPS may be co-located with the MME.

[0036] The means of the MME 13 illustrated in figure 6a for establishing the security key, K_eNB, comprises reception means 62 for receiving an NAS SERVICE REQUEST-message including an NAS_U-SEQ from a UE (via its serving eNodeB; key derivation means 63 for deriving a security key, K_eNB based on at least the received NAS _U-SEQ and a stored K_ASME, using a conventional key derivation function; and sending means 64 for sending the derived K_eNB to the eNodeB serving the UE.

[0037] Figure 6b illustrates a UE 11 (User Entity) according to this invention, the UE adapted for an EPS, and further arranged to establish a security key, K_eNB, for a security context for the protection of UP/RRC traffic exchanged with its serving eNodeB. The UE is provided with conventional communication means, not illustrated in the figure, for communicating with the nodes in the EPS via an LTE-Uu interface to its serving eNodeB.

[0038] The means of the UE 11 illustrated in the figure 6b for establishing the security key, K_eNB, comprises sending means 66 for sending an NAS SERVICE REQUEST-message to the MME, via the serving eNodeB, the request indicating an uplink sequence number, NAS_U-SEQ, and the means for establishing a security key, K_eNB, comprises key derivation means 67 for deriving a security key, K_eNB based on at least the NAS_U-SEQ and a stored K_ASME, using a conventional key derivation function.

[0039] The above-described means of the MME and the UE, as illustrated in the figures 6a and 6b, implement the described functions using a suitable combination of software and hardware, e.g. a programmed microprocessor or an application-specific integrated circuit, as well as conventional radio transmitters and receivers.

[0040] While the invention has been described with reference to specific exemplary realisations, the description is in general only intended to illustrate the inventive concept and should not be taken as limiting the scope of the invention.

Patentkrav

1. Fremgangsmåde i en mobilitetshåndteringsenhed (13) af et Evolved Packet System, EPS, til at etablere en sikkerhedsnøgle til beskyttelse af radioressourcestyrings-/brugerplantrafik mellem en brugerindretning (11), UE, og en radiobasestation (12), der betjener UE'en, hvilken fremgangsmåde omfatter følgende trin:
- At modtage (32, 52) en Non access Stratum-, NAS-, serviceanmodningsbesked fra UE'en, hvilken besked angiver et NAS uplink-sekvensnummer;
- At udlede (33, 53) sikkerhedsnøglen fra mindst det angivne NAS uplink-sekvensnummer og fra en lagret Access Security Management Entity-nøgle, der deles med UE'en, med anvendelse af en nøgleudledningsfunktion, der tager NAS uplink-sekvensnummeret og den lagrede Access Security Management Entity-nøgle som input;
- At videresende (34) den udledte sikkerhedsnøgle til radiobasestationen (12), der betjener UE'en.

2. Fremgangsmåde i en mobilitetshåndteringsenhed ifølge krav 1, hvor nøgleudledningsfunktionen er en Pseudo-Random Function.

3. Fremgangsmåde i en brugerindretning (11), UE, af et Evolved Packet System, EPS, til at etablere en sikkerhedsnøgle til beskyttelse af radioressourcestyrings-/brugerplantrafik udvekslet med en radiobasestation (12), hvilken fremgangsmåde omfatter følgende trin:
- At sende (31, 51) en Non access Stratum-, NAS-, serviceanmodning til en mobilitetshåndteringsenhed, hvilken besked angiver et NAS uplink-sekvensnummer;
- At udlede (33, 53) sikkerhedsnøglen fra mindst det angivne NAS uplink-sekvensnummer og fra en lagret Access Security Management Entity-nøgle, der deles med mobilitetshåndteringsenheden, med anvendelse af en nøgleudledningsfunktion, der tager NAS uplink-sekvensnummeret og den lagrede Access Security Management Entity-nøgle som input.

4. Fremgangsmåde i en UE ifølge krav 3, hvor nøgleudledningsfunktionen er en Pseudo-Random Function.

5. Fremgangsmåde i en UE ifølge et af kravene 3-4, omfattende det yderligere trin at beskytte integriteten af NAS-serviceanmodningen sendt til mobilitetshåndteringsenheden.

6. Fremgangsmåde i en UE ifølge et af kravene 3-5, omfattende trinnet med at lagre NAS uplink-sekvensnummeret eller angivelsen deraf af NAS-serviceanmodningen sendt til mobilitetshåndteringsenheden.

7. Fremgangsmåde i en UE ifølge et af kravene 3-6, hvor sikkerhedsnøglen udledes fra NAS uplink-sekvensnummeret og Access Security Management Entity-nøglen efter modtagelsen af en sikkerhedskonfigureringsbesked fra radiobasestationen.

8. Mobilitetshåndteringsenhed (13) af et Evolved Packet System, EPS, hvilken mobilitetshåndteringsenhed er indrettet til at etablere en sikkerhedsnøgle til beskyttelse af radioressourcestyrings-/brugerplantrafik mellem en UE (11) og en radiobasestation (12), der betjener UE'en, hvilken mobilitetshåndteringsenhed indbefatter

- Midler (62) til at modtage en Non access Stratum-, NAS-, serviceanmodningsbesked fra UE'en, hvilken besked angiver et NAS uplink-sekvensnummer;
- Midler (63) til at udlede sikkerhedsnøglen fra mindst det angivne NAS uplink-sekvensnummer og fra en lagret Access Security Management Entity-nøgle, der deles med UE'en, med anvendelse af en nøgleudledningsfunktion, der tager NAS uplink-sekvensnummeret og den lagrede Access Security Management Entity-nøgle som input;
- Midler (64) til at sende den udledte sikkerhedsnøgle til radiobasestationen (12), der betjener UE'en.

9. Mobilitetshåndteringsenhed ifølge krav 8, hvor nøgleudledningsfunktionen er en Pseudo-Random Function.

10. Brugerindretning (11), UE, af et Evolved Packet System, EPS, hvilken UE er indrettet til at etablere en sikkerhedsnøgle til beskyttelse af radioressourcestyrings-/brugerplantrafik udvekslet med en betjenende radiobasestation (12), hvilken UE indbefatter:
- Midler (66) til at sende en Non access Stratum-, NAS-, serviceanmodning til en mobilitetshåndteringsenhed, hvilken besked angiver et NAS uplink-sekvensnummer;
- Midler (67) til at udlede sikkerhedsnøglen fra mindst det angivne NAS uplink-sekvensnummer og fra en lagret Access Security Management Entity-nøgle, der deles med mobilitetshåndteringsenheden, med anvendelse af en nøgleudledningsfunktion, der tager NAS uplink-sekvensnummeret og den lagrede Access Security Management Entity-nøgle som input.

11. UE (11) ifølge krav 10, hvor nøgleudledningsfunktionen er en Pseudo-Random Function.

12. UE (11) ifølge et af kravene 10-11, omfattende det yderligere trin at beskytte integriteten af NAS-serviceanmodningen sendt til mobilitetshåndteringsenheden.

13. UE (11) ifølge et af kravene 10-12, omfattende trinnet med at lagre NAS uplink-sekvensnummeret eller angivelsen deraf af NAS-serviceanmodningen sendt til mobilitetshåndteringsenheden.

14. UE (11) ifølge et af kravene 10-13, hvor sikkerhedsnøglen udledes fra NAS uplink-sekvensnummeret og Access Security Management Entity-nøglen efter modtagelsen af en sikkerhedskonfigureringsbesked fra radiobasestationen.

DRAWINGS

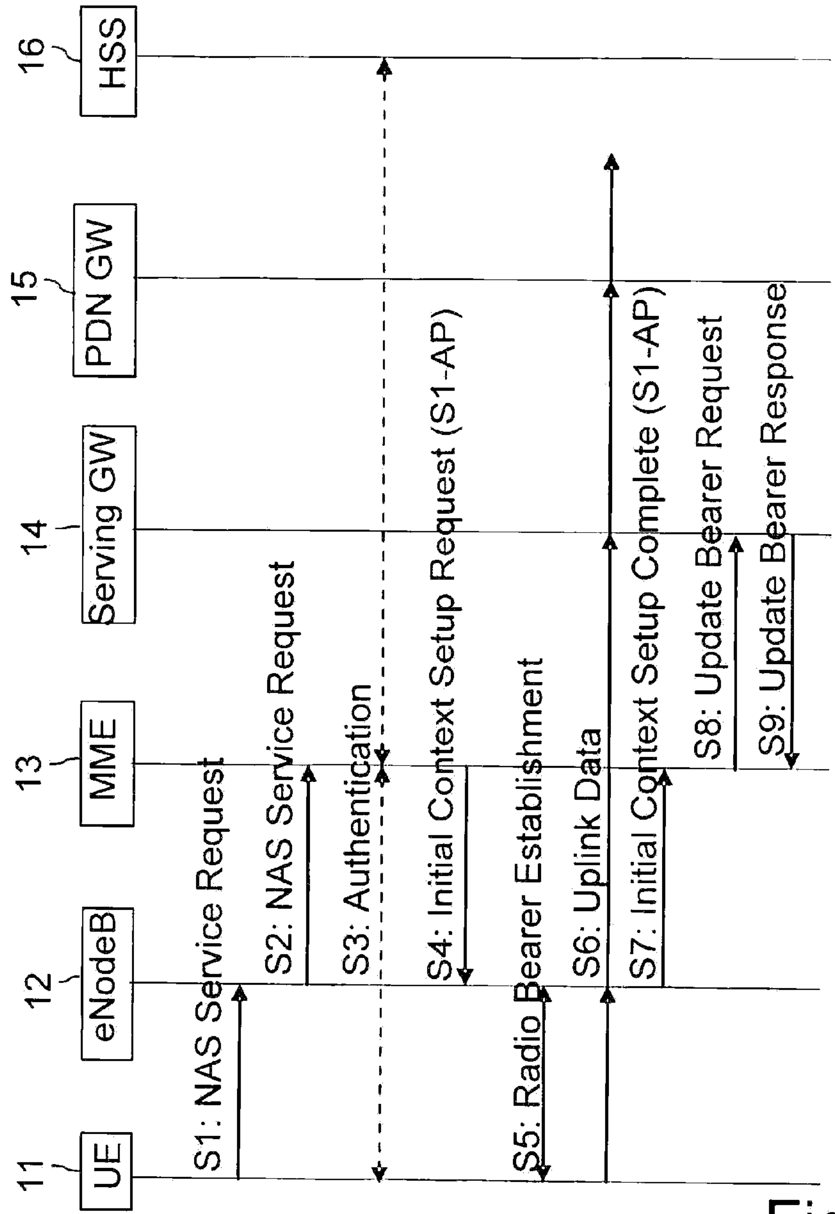

Fig. 1

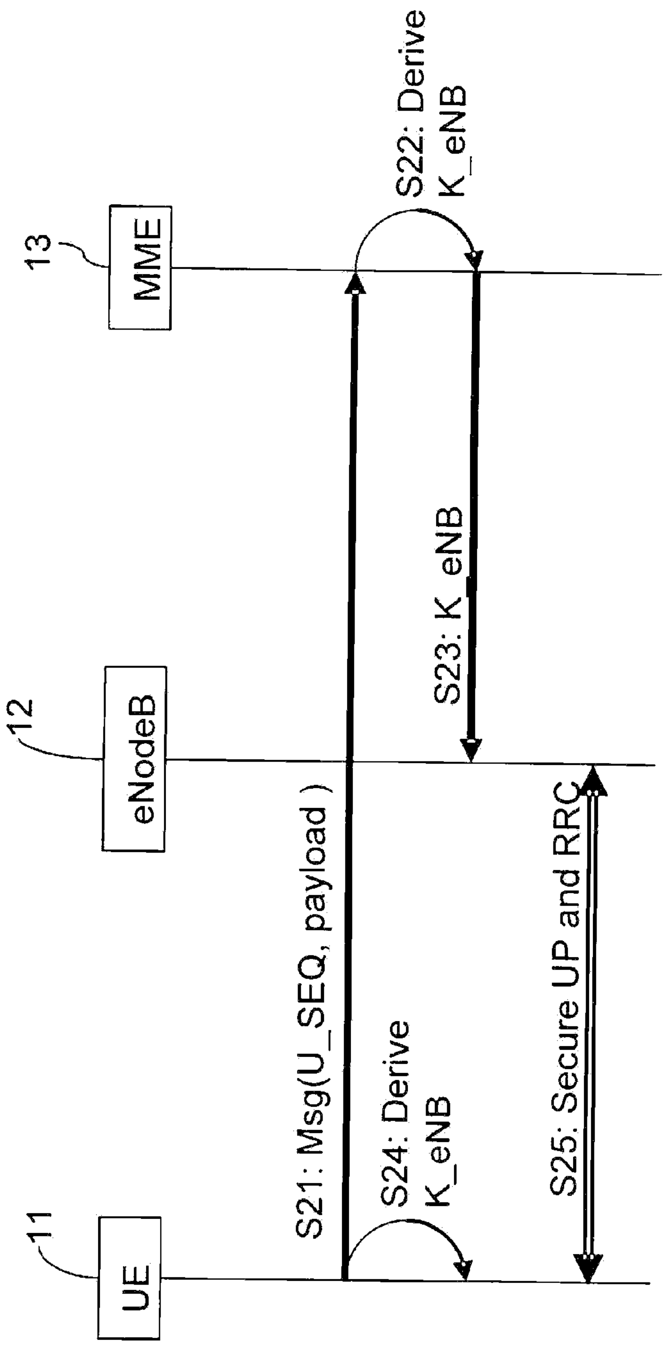
13
MME
12
eNodeB
11
UE
S21: Msg(U_SEQ, payload)
S22: Derive K_eNB
S23: K_eNB
S24: Derive K_eNB
S25: Secure UP and RRC

Fig. 2

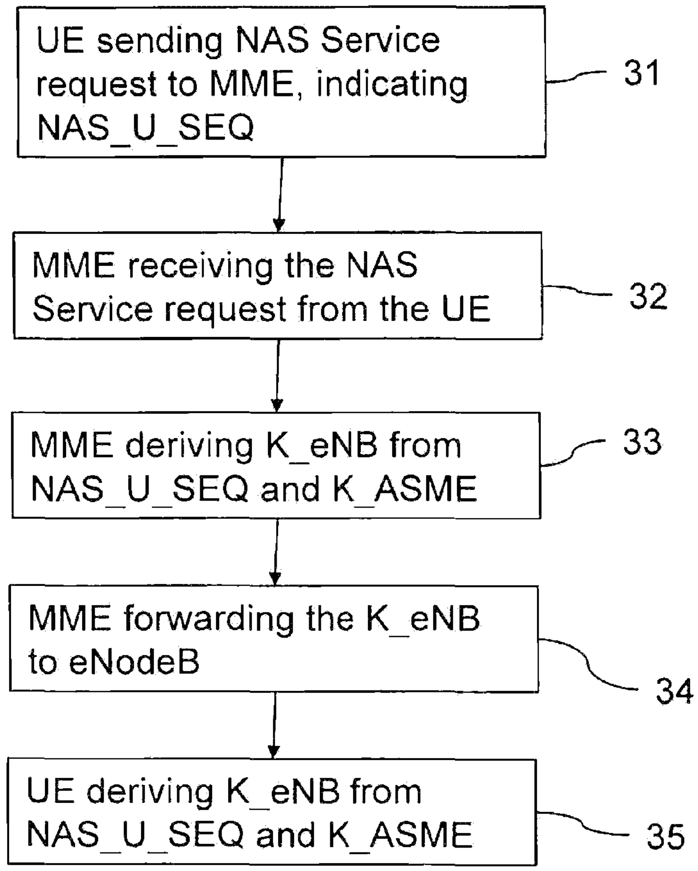
UE sending NAS Service request to MME, indicating NAS_U_SEQ
31
MME receiving the NAS Service request from the UE
32
MME deriving K_eNB from NAS_U_SEQ and K_ASME
33
MME forwarding the K_eNB to eNodeB
34
UE deriving K_eNB from NAS_U_SEQ and K_ASME
35

Fig. 3

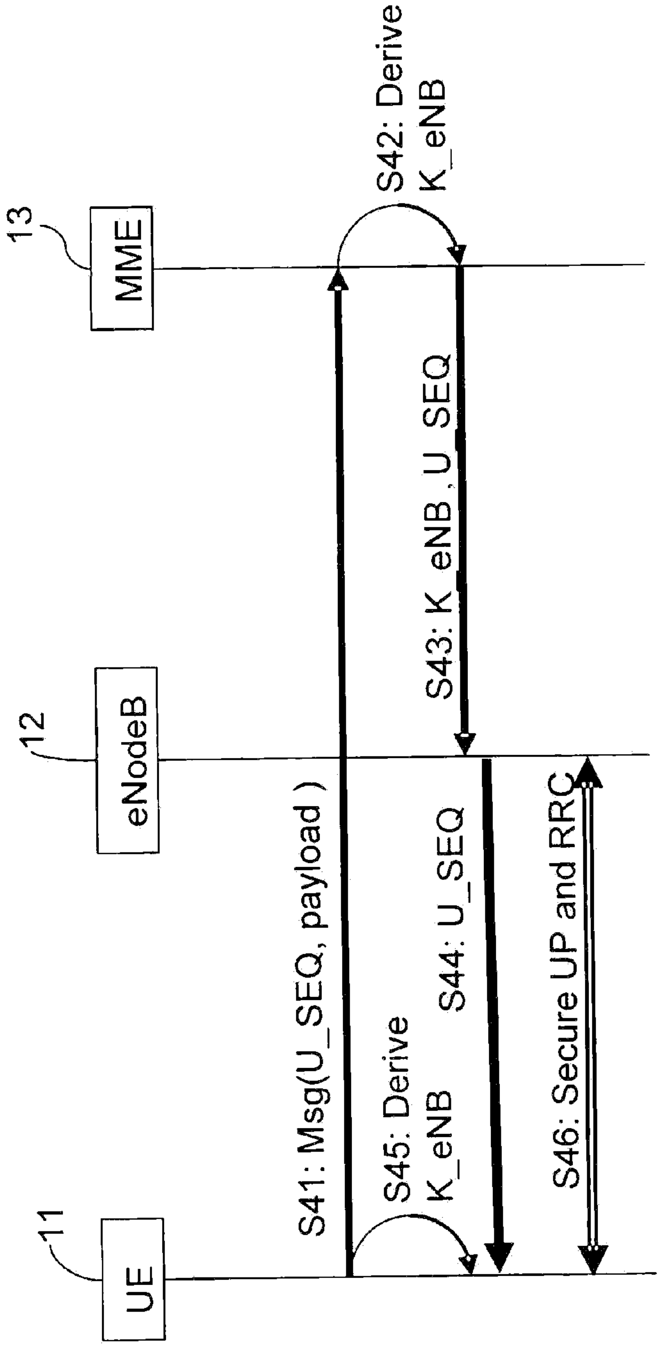
13
MME
12
eNodeB
11
UE
S41: Msg(U_SEQ, payload)
S42: Derive K_eNB
S43: K_eNB ,U_SEQ
S44: U_SEQ
S45: Derive K_eNB
S46: Secure UP and RRC

Fig. 4

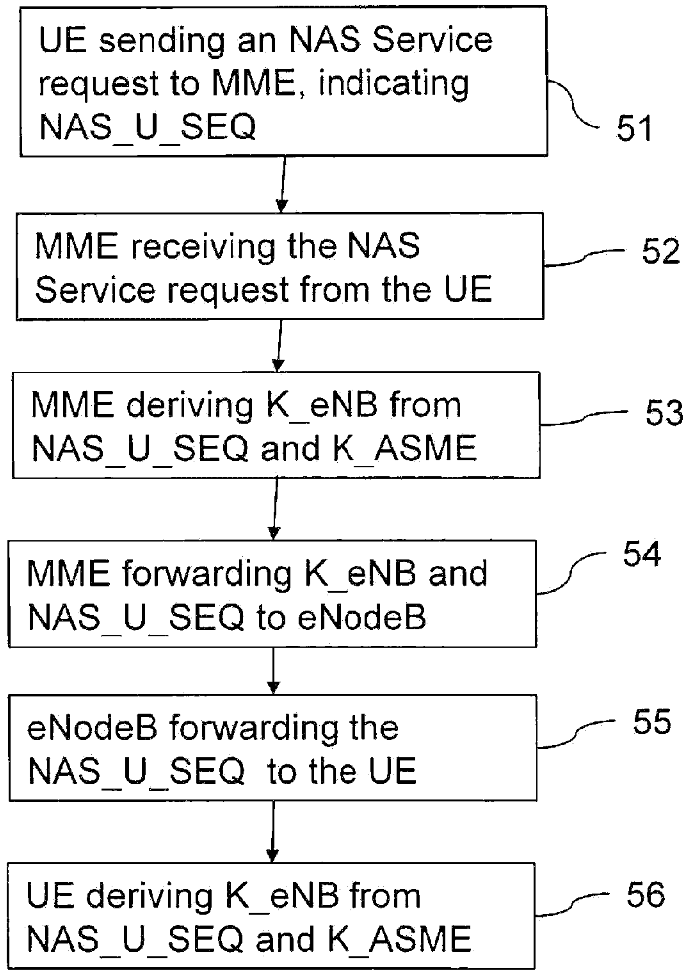
UE sending an NAS Service request to MME, indicating NAS_U_SEQ
51
MME receiving the NAS Service request from the UE
52
MME deriving K_eNB from NAS_U_SEQ and K_ASME
53
MME forwarding K_eNB and NAS_U_SEQ to eNodeB
54
eNodeB forwarding the NAS_U_SEQ to the UE
55
UE deriving K_eNB from NAS_U_SEQ and K_ASME
56

Fig. 5

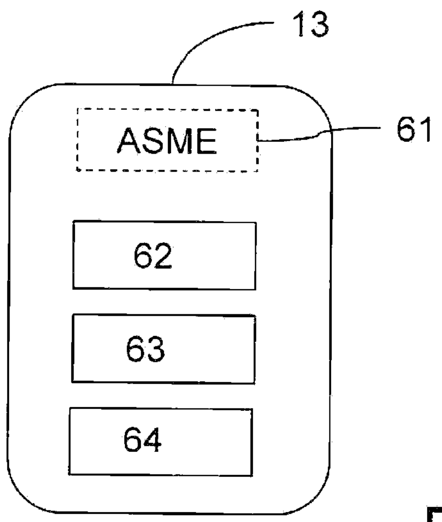

Fig. 6a

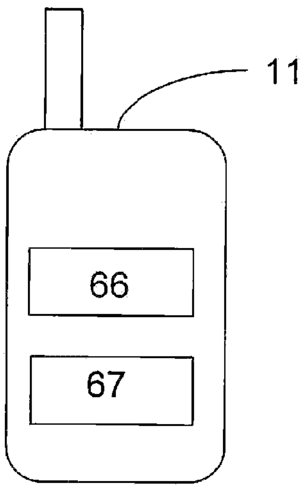

Fig. 6b