Internal distribution code:
(A) [ - ] Publication in OJ
(B) [ - ] To Chairmen and Members
(C) [ - ] To Chairmen
(D) [ X ] No distribution

Datasheet for the decision of 21 June 2016

Case Number: T 1890/13 - 3.5.05
Application Number: 08767152.5
Publication Number: 2191608
IPC: H04L9/08, H04L29/06, H04L9/32, H04W12/04
Language of the proceedings: EN

Title of invention:
Method and arrangement in a telecommunication system

Patent Proprietor:
Telefonaktiebolaget LM Ericsson (publ)

Opponent:
KELTIE LLP

Headword:
Generation of security keys/ERICSSON

Relevant legal provisions:
EPC Art. 56, 83, 87(1), 100(a), 100(b)
RPBA Art. 13(1)
Keyword:
Sufficiency of disclosure - (yes)
Validity of priority claim - (yes)
Admission of document substantiated only at the oral proceedings before the board - (no)
Inventive step - (yes)

Decisions cited:
Case Number: T 1890/13 - 3.5.05

DECISION
of Technical Board of Appeal 3.5.05
of 21 June 2016

Appellant: KELTIE LLP
(Opponent)
No. 1 London Bridge
London SE1 9BA (GB)

Representative: Lawrence, Richard Anthony
Keltie LLP
No. 1 London Bridge
London SE1 9BA (GB)

Respondent: Telefonaktiebolaget LM Ericsson (publ)
(Patent Proprietor)
164 83 Stockholm (SE)

Representative: Ericsson
Patent Development
Torshammsgatan 21-23
164 80 Stockholm (SE)

Decision under appeal: Decision of the Opposition Division of the European Patent Office posted on 2 July 2013 rejecting the opposition filed against European patent No. 2191608 pursuant to Article 101(2) EPC.

Composition of the Board:
Chair A. Ritzka
Members: K. Bengi-Akyuerek
D. Prietzel-Funk
Summary of Facts and Submissions

I. The appeal of the opponent is against the decision of the opposition division to maintain the present European patent as granted, in view of the invoked opposition grounds of lack of novelty and inventive step (Article 100(a) EPC in conjunction with Articles 54 and 56 EPC) and insufficient disclosure (Article 100(b) EPC in conjunction with Article 83 EPC).

II. The prior-art documents cited in the opposition proceedings and in the decision under appeal included the following:

D19: "Key refresh in SAE/LTE", 3GPP TSG SA WG3 Security - SA3#46b, S3-070234, pp. 1-6, March 2007;

D28: "Nonce-based key refresh on idle to active and detached to active transitions", 3GPP TSG SA WG3 Security - S3#48, S3-070530, pp. 1-4, July 2007;


III. With the statement setting out the grounds of appeal, the appellant requested that the decision under appeal be set aside and that the patent be revoked in its entirety on the grounds of insufficiency of disclosure (Article 100(b) EPC) and lack of novelty and inventive step (Article 100(a) EPC). Furthermore, it contended that the priority from US patent application

P1: US 60/972,955
was invalidly claimed with respect to the independent claims of the patent (Article 87(1) EPC).

IV. With a letter of reply dated 6 March 2014, the respondent filed amended claims according to seven auxiliary requests and requested that the appeal be dismissed (main request) or that the patent be maintained on the basis of the claims of any of the auxiliary requests. Furthermore, it requested that the ground of opposition under Article 100(a) EPC be rejected as inadmissible for lack of substantiation.

V. With a notice of intervention dated 19 August 2015, an intervener ("Apple Retail Netherlands B.V.") requested that the decision under appeal be set aside and that the patent be revoked in its entirety on the grounds of insufficiency of disclosure (Article 100(b) EPC) and lack of novelty and inventive step (Article 100(a) EPC). The intervener cited inter alia the following prior-art documents:


**HL4:** A. Menezes et al.: "Handbook of Applied Cryptography", chapters 9, 10 and 12, CRC Press, 1997.

VI. By a letter dated 22 December 2015, the intervener withdrew its intervention.

VII. With a letter dated 12 January 2016, the respondent filed additional sets of amended claims according to five further auxiliary requests (i.e. auxiliary request 7A and eighth to eleventh auxiliary requests).
VIII. In an annex to the summons to oral proceedings pursuant to Article 15(1) RPBA, the board expressed its preliminary opinion on the appeal. In particular, it made observations on the ground of insufficiency of disclosure, the validity of the priority claim, the admissibility of the claims of the auxiliary requests on file and the matter of novelty and inventive step, mainly having regard to documents D19, D29 and HL4.

IX. By a letter of reply, the respondent submitted observations on the board’s communication under Article 15(1) RPBA, in particular as regards the issue of novelty and inventive step in view of D19, D29 and HL4.

X. Oral proceedings were held on 21 June 2016, during which the matter of sufficiency of disclosure, the validity of the priority claim, the admission of D28 into the proceedings and the question of novelty and inventive step were discussed.

The appellant's final request was that the decision under appeal be set aside and that the patent be revoked.

The respondent's final request was that the appeal be dismissed or, alternatively, that the patent be maintained on the basis of the claims of auxiliary requests 1 to 7 submitted with the letter dated 6 March 2014 or of auxiliary requests 7A and 8 to 11 submitted with the letter dated 12 January 2016.

At the end of the oral proceedings, the decision of the board was announced.
XI. **Claim 1** of the patent reads as follows:

"A method in a Mobility Management Entity (13), MME, of an Evolved Packet System, EPS, of establishing a security key, K_enB, for protecting RRC/UP traffic between a User Equipment (11), UE, and an eNodeB (12) serving the UE, the method comprising the following steps:

- Receiving (32, 52) an NAS Service Request from the UE, the request indicating a [sic] NAS uplink sequence number, NAS_U_SEQ;
- Deriving (33, 53) the security key, K_enB, from at least said received NAS_U_SEQ and from a stored Access Security Management Entity-key, K_ASME, shared with said UE;
- Forwarding (34) said derived K_enB to the eNodeB (12) serving said UE."

Independent **claim 7** of the patent reads as follows:

"A method in a User Equipment (11), UE, of an Evolved Packet System, EPS, of establishing a security key, K_enB, for protecting RRC/UP traffic exchanged with a serving eNodeB (12), the method comprising the following steps:

- Sending (31, 51) a [sic] NAS Service Request to a Mobility Management Entity, MME, the request indicating a [sic] NAS uplink sequence number, NAS_U_SEQ;
- Deriving (35, 56) the K_enB from at least said NAS_U_SEQ and from a stored Access Security Management Entity-key, K_ASME, shared with said MME."
The further independent claims 13 and 18 of the patent are directed to corresponding apparatuses.

**Reasons for the Decision**

1. Independent claim 7 as granted, having the broadest scope among the granted independent claims, comprises the following features (as labelled by the board):

   A method in a User Equipment (UE) of an Evolved Packet System (EPS) of establishing a security key, K_eNB, for protecting Radio Resource Control/User Plane (RRC/UP) traffic exchanged with a serving eNodeB, the method comprising the following steps:

   A) sending a Non-Access Stratum (NAS) Service Request to a Mobility Management Entity (MME), the request indicating an NAS uplink sequence number NAS_U_SEQ;

   B) deriving the K_eNB from at least said NAS_U_SEQ and from a stored Access Security Management Entity (ASME) key, K_ASME, shared with said MME.

   The subject-matter of independent apparatus claim 18 as granted corresponds to that of claim 7, while independent claims 1 and 13 are directed to a method and apparatus respectively, further including the step of forwarding K_eNB from MME to the serving eNodeB.

   The independent claims are evidently based on the "first embodiment" of the opposed patent. That embodiment is concerned with generating the same security key K_eNB, which is subsequently used for securing traffic between UE and eNodeB, at both the user side ("UE") and the network side ("MME"), based on
security parameters such as NAS_U_SEQ and K_ASME, and forwarding the generated K_eNB to eNodeB (cf. paragraphs [0031] to [0037] in conjunction with Figures 2 and 3 of the opposed patent). The technical problem to be solved by those independent claims is to prevent replay attacks, without using complex sequence number estimation and synchronisation, or requiring explicit downlink NAS service accept messages from MME to UE (cf. paragraphs [0007] to [0011] of the opposed patent).

2. Sufficiency of disclosure (Article 83 EPC)

2.1 The appellant contended that, firstly, the independent claims as granted did not include the essential features of the patent's invention such as reuse of replay protection, integrity protected NAS messages and idle-to-active transitions of UE and that, secondly, the patent's specification did not provide the relevant standardisation information to enable a working implementation of the present invention.

2.2 The board, however, concurs with the opposition division and the respondent that the skilled person in the field of 3GPP-based mobile communications would know, without requiring further technical details, how to actually send transmission-specific parameters such as a sequence number ("NAS_U_SEQ") to another network device ("MME") and derive a security key from that transmission-specific parameter and another security key ("K_ASME") according to the features of the independent claims as granted.

2.3 The appellant did not present any further arguments or comments at the oral proceedings before the board.
3. **Validity of priority claim (Article 87(1) EPC)**

3.1 It is apparent to the board that priority document **P1** directly and unambiguously discloses feature A), i.e. sending an NAS service request message "Msg" including an NAS uplink sequence number "U_SEQ" (see e.g. Fig. 2: "Msg(U_SEQ, payload)");, and feature B), i.e. deriving a security key "K_eNB" to be used for protecting RRC/UP traffic exchanged between UE and the serving eNodeB from at least U_SEQ and a shared "K_ASME" (see e.g. Fig. 2: "Derive K_eNB = PRF (U_SEQ, K_ASME, ...)").

Hence, priority document P1 obviously discloses the "same invention" in the sense of Article 87(1) EPC. Consequently, the effective filing date of the opposed patent is taken to be 17 September 2007.

3.2 The appellant did not provide any further arguments or comments at the oral proceedings before the board.

4. **Novelty and inventive step (Articles 54 and 56 EPC)**

At the oral proceedings before the board, the appellant did not challenge the novelty of the opposed patent's independent claims (Article 54 EPC). For the purpose of attacking inventive step, the appellant relied essentially on three prior-art documents, namely **D28**, **D19** and **D29**. Since the appellant first requested that D28 be introduced into the appeal proceedings, this issue was discussed and decided first.

4.1 **Admission of D28 as substantiated into the appeal proceedings**

4.1.1 Document **D28** was initially filed with the notice of opposition. Thus, it was filed in due time within the
meaning of Article 114(2) EPC. However, it was discussed neither during the oral proceedings before the opposition division nor in the impugned decision.

4.1.2 As regards appeal proceedings, Article 12(2) RPBA clearly states that the statement setting out the grounds of appeal or the corresponding reply shall contain a party's complete case, and in particular should specify expressly all the facts, arguments and evidence relied on.

4.1.3 Concerning substantiation of the filing of D28, the statement setting out the grounds of opposition made the following reference to it (cf. page 11, second paragraph, third sentence; emphasis added by the board):

"Documents D27, D28 and D29 provide specific proposals for consideration. D27 and D28 develop the D23 and D24 approaches respectively ...",

while the statement setting out the grounds of appeal (cf. page 6, last paragraph, third sentence; emphasis added by the board) includes the following statement:

"D19 provides a worked-out scheme for managing key refresh in transitions ... and discusses a number of alternative approaches for providing nonce or counter (as noted in D28, a counter is merely a specific example of a nonce) data to achieve key refresh."

The board concurs with the respondent that this kind of incidental citation of D28 within a line of argument in support of lack of patentability amounts to mentioning a prior-art document merely as background information
for standardisation developments, but fails to deliver any information as to whether it is intended to be used, for example, as a starting point for attacking inventive step or as evidence of common general knowledge or anything else. Moreover, no specific passage of D28 had been cited in the written procedure. Thus, D28 remained unsubstantiated throughout the entire written proceedings.

It was only at the oral proceedings before the board that the appellant argued for the very first time that D28 constituted a development of 3GPP-based standardisation documents such as D19, and that it was extremely relevant for the assessment of inventive step, since it demonstrated on page 2, first paragraph, that a number used only once, i.e. "NonceUE", could indeed be derived from a counter, i.e. "CountNASint" here. Hence, this new line of argument based on D28 was submitted after the appellant had filed its statement setting out the grounds of appeal and after the board had arranged oral proceedings, i.e. at a very late stage in the overall proceedings. Therefore, the question of admitting the substantiated document D28 into the appeal proceedings is subject to Article 13(1) and (3) RPBA in the present case.

4.1.4 In the light of the above and in accordance with the respondent's request, the board decided to exercise its discretionary power to refuse the appellant's request that D28 be introduced into the appeal proceedings under Article 13(1) RPBA, for the following reasons:

- the late substantiation of D28 was not an appropriate and immediate reaction to unforeseeable developments in the proceedings which did not lie in the responsibility of the
appellant, rather it was submitted by the appellant entirely of its own volition;
- the teaching of D28 was not *prima facie* more relevant than the other prior-art documents on file or highly likely to prejudice the maintenance of the opposed patent, since the use of a counter for NAS integrity protection, i.e. Count\textsubscript{NAS\text{int}}, in no way corresponds to a sequence number associated with uplink transmissions of NAS service request messages as claimed;
- admitting into the appeal proceedings such a new line of argument based on D28 would run counter to the principle of procedural economy and fairness.

4.2 *Document D19 as closest prior art*

The teaching of **D19** is concerned with key refresh procedures in 3GPP-based mobile networks such as LTE (Long-Term Evolution) systems. More specifically, it discloses UE-initiated updates of K\_eNB, which is derived at least from two random *numbers used only once*, namely Nonce\textsubscript{UE} and Nonce\textsubscript{SN}, and K\_ASME (see page 2, section 2.1, fourth item). Nonce\textsubscript{UE} is supposed to be generated by UE and sent to MME via eNodeB in an initial layer-3 message, whereas Nonce\textsubscript{SN} is generated by MME (see e.g. Figure 1). The board agrees with the decision under appeal that the sole difference between the independent claims as granted and the disclosure of D19 is that

1) the number used for deriving K\_eNB at UE and MME is an *NAS uplink sequence number* (rather than a random number like Nonce\textsubscript{UE});
ii) the NAS uplink sequence number is indicated to MME in an **NAS service request** sent from UE to MME.

### 4.2.1 Technical effect of features i) and ii)

The board also accepts that the above distinguishing features yield the technical effect that NAS-based key security upon idle-to-active transitions is maintained without the need for any feedback signal from MME, i.e. from the network side, such as an "NAS service accept" message or a downlink sequence number (see e.g. paragraph [0011] of the opposed patent). Hence, the board sees the objective technical problem to be solved as "how to maintain replay protection in the 3GPP-based network of D19, when no explicit feedback from the network side is foreseen".

### 4.2.2 Non-obviousness of the subject-matter claimed

Firstly, the board concurs with the conclusion in the appealed decision that the use of an NAS service request constitutes a typical example of an "initial layer-3 message" and hence cannot contribute to inventive step.

Secondly, the board holds that the skilled person in the field of 3GPP-based mobile communications would also be aware that a message sequence number *could*, in principle, be used as a nonce (see e.g. **HL4**, page 398, item 3: "To uniquely identify a message or sequence of messages ..., nonces drawn from a monotonically increasing sequence may be used ..." and page 399, section 10.12(ii), first sentence: "A sequence number ... is typically used to detect message replay ..."). In this regard, the appellant argued that the claimed solution was obvious merely because the
possibility of using sequence numbers as a key
derivation parameter already existed at the patent's
effective filing date.

The board notes however that the decisive question is
rather whether the skilled person would indeed apply a
sequence number for uplink NAS messages as a nonce
generated by UE, i.e. Nonce_{UE}, in the system described
in D19. Put differently, the pivotal question for the
present inventive-step assessment is not whether a
nonce could under certain circumstances be a counter,
as the appellant repeatedly argued, but whether it
would be obvious that this nonce corresponds to a very
specific message sequence number, namely NAS_U_SEQ. In
this context, it is first apparent to the board that
D19 - despite expressly mentioning that encryption and
integrity protection relied *inter alia* on "counters or
sequence numbers" (see page 1, first paragraph, second
sentence) - fails to provide an explicit or implicit
indication as to the usability of such a sequence
number as Nonce_{UE}. On the contrary, it stresses that it
is desirable that counters are to be stored only on the
network side, i.e. at MME (see page 2, first paragraph,
second sentence).

Furthermore, when analysing Figure 1 of D19, the
skilled person would immediately discern that the main
feedback provided by MME is formed by a "security mode
command" message, which in turn carries the relevant
NAS security context parameters. Accordingly,
confronted with the above-identified objective problem,
the skilled person would be well aware - regardless of
whether or not the security mode command of D19 can be
equated with any "NAS service accept" message
whatsoever as quoted in the opposed patent - that, if
no security mode command is sent as feedback signal
from MME, no nonce (such as NonceSN) generated by MME and required for deriving K_eNB could self-evidently be sent from MME either. The board agrees with the respondent that in such a situation the skilled person would rather dispense with the second nonce (i.e. NonceSN) produced by MME than resort to the use of a counter associated with an uplink sequence number at the user side. Thus, the skilled person would apply only a single nonce, namely NonceUE, as an input parameter for the generation of K_eNB, particularly since using counters (for counting message sequence numbers) is generally construed to be a more complex solution and thus a technical drawback according to the teaching of D19 (see e.g. page 1, last paragraph, second sentence). In summary, the board concludes that arriving at the derivation of K_eNB from an uplink sequence number of NAS service request messages as claimed would be possible only by extrapolating the teaching of D19 with impermissible hindsight.

4.3 Document D29 as closest prior art

The disclosure of D29 is directed to a more efficient re-keying scheme proposed for 3GPP-based mobile networks (LTE networks). In particular, it relies on network-initiated updates of K_eNB to be derived at UE and MME at least from a newly proposed key K_MME and a counter value relating to downlink transmissions of NAS messages, named "LSB_NAS_counter" (see page 2, last paragraph). That counter is sent from MME to UE via eNodeB in a security mode command message ("NAS SMC"). Contrary to the finding in the decision under appeal (see reasons 2.3.4), the board agrees with the appellant that D29 also teaches that an NAS service request message is to be sent from UE to MME (see D29, page 4, section entitled "Effect of proposal on Service
Request message”, last sentence). In addition, according to D29, a counter for transmissions of uplink NAS messages, i.e. “LSB_NAS_counter (uplink)”, is only sent in an NAS response message (see page 3, third full paragraph: "The response part of the NAS SMC consists of the LSB_NAS_counter (uplink) and the NAS_MAC ...”). Hence, the board takes the view that the independent claims as granted differ from the disclosure of D29 in that

iii) the counter value used for deriving K_eNB at UE and MME is an NAS uplink sequence number (rather than an NAS downlink sequence number);
iv) the NAS uplink sequence number is indicated to MME in an NAS service request message (rather than in an NAS SMC response message) sent from UE to MME.

4.3.1 Technical effect of features iii) and iv)

As regards the technical effect of those distinguishing features, the opposed patent (cf. paragraph [0007]) contains the following teaching in relation to the conventional 3GPP-based key generation scheme as depicted in Figure 5.3.4-1 on page 40 of HL3 and in Figure 1 of the patent:

"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 ... 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."

The board concludes that the objective problem as formulated in point 4.2.1 above still applies when starting from D29 as closest prior art. A formulation of the objective problem such as "how to provide an efficient key exchange based on sequence numbers", as invoked by the appellant at the oral proceedings before the board, cannot be accepted since it evidently includes a pointer towards its actual solution.

4.3.2 Non-obviousness of the subject-matter claimed

As to distinguishing feature iii), the appellant argued that the following teaching of D29 provided a clear hint towards using an uplink sequence number as an input parameter for the subsequent derivation of K_eNB (see page 4, sub-section "General", second paragraph; emphasis added by the board):

"The proposed method also allows a simple method of a **UE initiated** key change, if such a case is desired in SAE/LTE. The UE would send a **message** consisting of the KSI of its current K_{ASME} and **UE_nonce** to the MME and the MME can then initiated[sic] a security mode command to change the keys. It also provides a method of generating a new K_{eNB} from a K_{MME} during an eNode handover with an MME change."

However, the appellant failed in the written and oral proceedings to convincingly and cogently demonstrate that
- a "UE-initiated key change" according to D29 necessarily implies that a sequence number for uplink messages is sent for key derivation purposes from UE to MME;
- the sent "message" in D29 constituted an NAS service request message;
- the "UE_nonce" sent together with the KSI (Key Set Identifier) of K_ASME from UE to MME in that message had to include NAS_U_SEQ by analogy with the network-initiated case (where the sequence number for downlink messages, i.e. NAS_D_SEQ, is transferred and used for the derivation of K_eNB).

Instead, the board believes that the skilled person would understand from the above passage in combination with the overall teaching of D29 that a user-initiated key change merely implies sending a first message (whose equivalence with an NAS service request message, in the absence of any further details about the type or purpose of such a message, is mere speculation) from UE to MME rather than from MME to UE upon an idle-to-active transition, and that it is still the network side (i.e. the MME) which has to initiate a refresh of K_eNB via a security mode command (SMC) message based on the relevant input parameters NAS_D_SEQ and K_MME.

Concerning distinguishing feature iv), D29 teaches that the service request message may contain a message authentication code "NAS_MAC" for integrity protection purposes and an "associated counter" (cf. page 4, penultimate paragraph). However, the board subscribes to the respondent’s view that said associated counter relates in fact to the current state of the counter for NAS integrity protection rather than to a counter for
sequentially sent uplink NAS messages, i.e. NAS_U_SEQ (see also appealed decision, reasons 2.3.5).

The appellant's further argument that the skilled person would readily apply the transmission of NAS_U_SEQ within NAS service request messages, if the size constraints with regard to such messages according to D29 (see e.g. sections entitled "Effect of proposal on Service Request message" and "Conclusion") no longer applied, must likewise fail. In fact, D29 merely proposes to dispense with the transmission of the UE security capabilities and the corresponding Key Set Identifiers (KSIs) in order to comply with the requirement of reduced message size (see in particular the section entitled "Effect of proposal on Service Request message", fourth and fifth paragraphs). In view of the above, the board concludes that the skilled person would in fact be dissuaded from applying the claimed solution in the system of D29, especially given that D29 likewise points out that the use of counters is considered a complicated implementation measure because it introduces possible error cases in keeping them synchronised (see page 1, first paragraph, last sentence).

4.4 In view of the analysis made in points 4.2 and 4.3 above, the board holds that, even if the teachings of D19 and D29 were combined, the skilled person would not arrive at the solution claimed. Hence, in the light of the prior art cited and discussed, the subject-matter of the independent claims as granted is new and involves an inventive step within the meaning of Articles 54 and 56 EPC.

5. In conclusion, since none of the opposition grounds invoked is found to prejudice the maintenance of the
patent as granted, the appeal has to be dismissed, and the present auxiliary claim requests need not be considered further.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chair:

P. Martorana A. Ritzka

Decision electronically authenticated