Internal distribution code:

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

Datasheet for the decision of 27 June 2017

Case Number:	T 1082/14 - 3.5.05
Application Number:	04775405.6
Publication Number:	1671511
IPC:	H04L9/08, H04L9/32, H04L29/06, H04W12/02, H04W12/04
Language of the proceedings:	EN

Title of invention:
ENHANCED SECURITY DESIGN FOR CRYPTOGRAPHY IN MOBILE COMMUNICATION SYSTEMS

Patent Proprietor:
Telefonaktiebolaget LM Ericsson (publ)

Opponent:
KELTIE LLP

Headword:
Algorithm specifc AKA key modification/ERICSSON

Relevant legal provisions:
EPC Art. 54, 56, 83, 84, 87

This datasheet is not part of the Decision.
It can be changed at any time and without notice.

Keyword:

Priority - (yes)
Claims - clarity (yes)
Sufficiency of disclosure - (yes)
Novelty - (yes)
Inventive step - (yes)

Decisions cited:

G 0003/14, G 0002/98

Catchword:

This datasheet is not part of the Decision.
It can be changed at any time and without notice.

Europäisches Patentamt
European Patent Office
Office européen des brevets

Beschwerdekammern
Boards of Appeal
Chambres de recours

European Patent Office
D-80298 MUNICH
GERMANY
Tel. +49 (0) 89 2399-0
Fax +49 (0) 89 2399-4465

Case Number: T 1082/14 - 3.5.05

DECISION
# of Technical Board of Appeal 3.5.05
of 27 June 2017

Appellant:
(Opponent)

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

Representative:

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

Respondent:
(Patent Proprietor)

Telefonaktiebolaget LM Ericsson (publ)
164 83 Stockholm (SE)

Representative:

Röthinger, Rainer
Wuesthoff & Wuesthoff
Patentanwälte PartG mbB
Schweigerstrasse 2
81541 München (DE)

Decision under appeal:

Interlocutory decision of the Opposition Division of the European Patent Office posted on 14 March 2014 concerning maintenance of the European Patent No. 1671511 in amended form.

Composition of the Board:

Chair A. Ritzka
Members: P. Cretaine
F. Blumer

Summary of Facts and Submissions

I. This appeal is against the interlocutory decision of the opposition division, dispatched on 14 March 2014, to maintain European patent No. 1 671 511 in amended form according to a Main Request filed during the oral proceedings on 29 January 2014. The opposition was based on the grounds of Article 100(a) and (b) EPC.

The opposition division found that independent claims 1, 18, 30 and 33 of the Main Request were entitled to the priority of the first application:

D7: US provisional patent application No. 60/505/748.

The opposition division decided that the opposed patent fulfilled the requirements of Article 83 EPC and that the subject-matter of the claims according to the Main Request was novel (Article 54 EPC) and involved an inventive step (Article 56 EPC) having regard to the prior art disclosed in:

D4: Barkan, Biham & Keller, "Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication", Proceedings of Crypto 2003, 17 to 21 August, 2003, provided in the form published as Technical Report CS-2003-05 of the Technion Computer Sciences Department,

D5: S3-030463 "Cipher key separation for A/Gb security enhancements", provided by Vodafone for discussion in 3GPP TSG SA WG3 Security on 15 to 18 July 2003 (documents publicly available from 3GPP),

D18: A. Menezes et al.: "Handbook of Applied Cryptography", Chapter 13, CRC Press, 1996, D19: M. Horowitz: "Key Derivation for Authentication, Integrity, and Privacy", Internet Draft for Network Working Group made publicly available in August 1998,

D20: H. Krawczyk: "SKEME: a versatile secure key exchange mechanism for Internet", Proceedings of the Symposium on Network and Distributed System Security, 1996, pages 114 to 127, presented on 22 to 23 February 1996,

D21: D. Wagner and B. Schneier: "Analysis of the SSL 3.0 protocol", the Second USENIX Workshop on Electronic Commerce Proceedings, USENIX Press, November 1996, pages 29 to 40,

D22: T. Dierks and C. Allen: "The TLS Protocol Version 1.0", RFC2246 for Network Working Group made publicly available in January 1999,

D24: WO 03/015360,

D25: WO 02/100065,

D26: D. Harkins and D. Carrel: "The Internet Key Exchange (IKE)", RFC2409 for Network Working Group made publicly available in November 1998,

D30: S3-030542, "Enhancements to GSM/UMTS AKA", Ericsson, discussed in meeting #30 of 3GPP SA WG3, and

D32: draft-ietf-secsh-transport-14.txt, published on 20 March 2002.

II. The opponent's notice of appeal was received on 13 May 2014 and the appeal fee was paid on the same day. The statement setting out the grounds of appeal was received on 11 July 2014. The opponent (appellant) requested that the decision be set aside and that the patent be revoked on the grounds of Article 100(a) and (b) EPC, and further because the claims as amended lacked clarity (Article 84 EPC). In particular the opponent objected that the claims as granted and as amended during opposition proceedings were not entitled to the priority date of the first application D7. Oral proceedings were requested on an auxiliary basis.

III. By letter dated 19 January 2015, the proprietor (respondent) responded to the opponent's statement setting out the grounds of appeal. The proprietor requested that the opponent's appeal be dismissed and that the patent be maintained according to the Main Request underlying the decision. It also submitted new sets of claims according to Auxiliary Requests I to IV and requested oral proceedings as a further auxiliary measure.

IV. A summons to oral proceedings was issued on 11 April 2017. In an annex to the summons, the board indicated the points which would be discussed during the oral proceedings. The board also expressed its preliminary opinion that the claims according to the Main Request were entitled to the priority of the first application D7, that the objection under Article 84 EPC against the Main Request was not admissible, and that the opposed patent fulfilled the requirements of Article 83 EPC.

V. By letter dated 26 May 2017, the proprietor responded to the summons and provided further arguments in favour of its requests.

VI. During the oral proceedings held before the board on 27 June 2017, the proprietor submitted a set of claims according to Auxiliary Request 1.

VII. The opponent requested that the decision under appeal be set aside and that European patent No. 1 671 511 be revoked.

VIII. The proprietor requested that the decision under appeal be set aside and that the patent be maintained on the basis of the main request, filed as Auxiliary Request 1 during oral proceedings before the board, or, subsidiarily, on the basis of any of Auxiliary Requests I to IV as filed with letter dated 19 January 2015.

At the end of the proceedings, the decision of the board was pronounced.

IX. Claim 1 of the main request (filed as Auxiliary Request 1 during oral proceedings before the board) reads as follows:

"A method of enhancing security for protected communication based on a key agreement procedure (S1) in a mobile communications network serving a mobile terminal (100) having at least one basic cryptographic security algorithm, said method comprising the steps of:
- selecting, on a network side, an enhanced version of a basic cryptographic security algorithm for communication between the mobile terminal and the network side (S2);
- transmitting, from the network side, information representative of the selected algorithm to the mobile terminal,

- modifying a basic security key resulting from the key agreement procedure in dependence on information representative of the selected algorithm to generate an algorithm-specific security key (S3);
- applying the basic cryptographic security algorithm with the algorithm-specific security key as key input to enhance security for protected communication in said mobile communications network (S4)."

The main request comprises further independent claims directed to a corresponding arrangement (claim 19), and to a mobile terminal (claim 30) and a network node (claim 33) adapted to perform, in cooperation, the method of claim 1.

Due to the outcome of the appeal procedure, there is no need to detail the claims according to the auxiliary requests.

Reasons for the Decision

1. Admissibility of the appeal

The appeal of the opponent complies with the provisions of Articles 106 to 108 EPC (cf. point II above) and is therefore admissible.

2. Admissibility of the main request (filed as Auxiliary Request 1 during oral proceedings before the board)

The opponent objected in its statement setting out the grounds of appeal that the change from the wording "network node" in the granted claims to the wording "network side" in claims 33 to 36 as maintained by the opposition division introduced a lack of clarity in respect of the functional elements involved. In response, the proprietor submitted during the oral proceedings a set of claims according to Auxiliary Request 1, wherein the wording "network node" has been reinstated in claims 33 to 36.

The board, in view of the limited complexity and scope of the amendments introduced by Auxiliary Request 1, has exercised its discretion and decided under Article 13(1) RPBA to admit this request into the appeal proceedings.

3. Validity of priority right - Article 87 EPC

3.1 The opponent has challenged the validity of the priority claim. In this context the board noted that the opponent did not explain in the statement setting out the grounds of appeal why in its view the findings of the opposition division could not be followed, contrary to the requirements of Article 12(2) RPBA. However, in view of the low complexity of this issue, from both a technical and a legal point of view, the board exercised its discretion according to Article 13(1) RPBA, and decided in oral proceedings that the priority issue could be part of the subject-matter of the appeal proceedings.

3.2 The opponent contended that four features present in the independent claims as maintained by the opposition division, and still present in the claims according to the main request, were not taught by priority document D7.

Firstly, the opponent argued that D7 did not teach that the protected communication was based <u>on a key agreement procedure in a mobile communication network</u>

but rather on an AKA (Authentication and Key Agreement) key agreement for GSM specifically. The board is not convinced by this argument since D7 clearly considers the GSM network as an example only of a mobile communication network in which the invention can be implemented (see D7, page 1, lines 6 to 8: "more particularly"; page 2, lines 23 to 28: "such as GSM"; page 3, lines 21 to 25: "not only in GSM but also in UMTS, CDMA or future generation systems"; page 3, lines 27 to 28: "in e.g. the GSM/UMTS AKA procedures"; page 6, lines 5 to 7: "such as GSM"). From these passages it is clear that D7 is concerned with mobile communication networks in general and standard key agreement procedures in these networks.

Secondly, the opponent contended that D7 did not provide support for the provision of an enhanced version of a cryptographic security algorithm. However, the board notes that D7 discloses (see page 3, lines 5 to 13; page 5, lines 24 to 26; Figure 2, step 2) that the original ciphering algorithm is updated, which means in substance that the basic version of the cryptographic algorithm is converted to an enhanced version, in full accordance with the wording used in the claims.

Further, the opponent objected that the feature of modifying a basic security key was more general than the specific teaching of D7 of using a one-way function to modify an original key. The board finds this assertion incorrect since D7 uses the generic term "modification" to define the operation performed on the key that was used in the original algorithm, i.e. on the basic security key (see page 3, lines 5 to 7 and 10 to 12; page 5, line 25).

Lastly, the opponent asserted that the feature "information representative of the selected algorithm" was more general than the specific disclosure in D7 of an algorithm identifier. The board however agrees with the proprietor that the teaching of D7 on page 5, lines 21 to 28, in particular the use of the wording "a value identifying the algorithm selected by the network", clearly supports a key modification in dependence on information representative of the algorithm.

Moreover, the opponent argued that the language used for defining features in the first application was not used, or mirrored, in the application claiming priority. The board is not convinced by this argument since G 2/98, which set out the requirement for claiming priority of the "same invention", does not demand that the language used be identical in the two applications.

For these reasons, the board judges that the main request is entitled to the priority of the first application D7 (Article 87 EPC).

4. Clarity - Article 84 EPC

The opponent raised clarity objections against claim 1 as maintained by the opposition division. Some of these objections were directed to the following features which are still present in claim 1 according to the main request:

- "...*enhanced version of a basic cryptographic security algorithm*",
- "...*modifying a basic security key resulting from the key agreement procedure*...",

- "...*in dependence on information representative of the selected algorithm to generate an algorithm-specific security key (S3)*",
- "...*applying the basic cryptographic security algorithm with the algorithm-specific security key as key input to enhance security for protected communication in said mobile communication network*".

In accordance with the case law of the boards of appeal, a clarity objection against a claim which has been amended during the opposition procedure, which is the case for claim 1 as maintained, may be raised only when, and then only to the extent that, the amendment introduces non-compliance with Article 84 EPC (see G 3/14). However, the above-mentioned four features were already literally present in claim 1 as granted.

The board therefore decided not to admit the clarity objection based on these four features into the appeal proceedings.

5. Main request - novelty

5.1 Since it has been decided that the priority claim is valid (see section 3), document D30 published after the priority date is not part of the prior art according to Article 54(2) EPC.

5.2 D32

The opponent first argued that the subject-matter of claim 1 was already disclosed in section 5 of D32, which describes a key exchange protocol for deriving session keys between a client and a server.

D32 relates to the SSH protocol working over the internet protocol. Section 5.1 discloses in paragraph "encryption algorithms" that a list regarding supported algorithms is first exchanged between the server and the client and that the first algorithm on the client's list that is also on the server's list is chosen as encryption algorithm. Further, section 5.2, third paragraph, describes how the client-to-server encryption key for the chosen algorithm is generated as the result of a HASH function. This function operates on the parameters K, H, C and a session-id. K is a shared secret, C is the single character C in ASCII and H is itself based on a value SSH_MSG_KEXINIT (see section 6, fifth paragraph on page 15). This last value itself is defined (see section 5.1, first paragraph) as including all the names of the algorithms listed on the lists. None of the parameters K, H, C and session_id is thus specific to the selected algorithm.

From this analysis of D32 it follows that, contrary to what was asserted by the opponent, the algorithm is not selected by the network side, i.e. the server, and that the encryption key is not specific to the selected algorithm.

For at least these two reasons, the subject-matter of claim 1 is novel over the teaching of D32.

5.3 D5

The opponent further argued that the subject-matter of claim 1 was already disclosed in D5. D5 teaches to reserve a bit mask in the RAND value sent by the base station in GSM authentication protocols to indicate which cryptographic algorithms may be used by the mobile station, for instance by using a bit mask with zeros in every position except for one identifying the selected A5 encryption algorithm. It is thus ensured that the Kc key generated during the authentication and AKA key agreement procedure will be used only in connection with the particular algorithm signalled in the modified RAND, achieving a certain level of key separation. According to the opponent, D5 teaches that the basic security key, which would result from the conventional RAND in which each bit is random, is modified in D5 by virtue of the specific RAND to become specific to the selected algorithm.

However, as correctly pointed out by the proprietor, the approach taught by D5 generates a single key, K_C, whereas the method according to claim 1 generates a first key according to a key agreement procedure and then modifies it to generate a second key used for encryption.

Therefore, for at least this reason, the subject-matter of claim 1 is novel over the teaching of D5.

5.4 The board thus judges that claim 1 according to the main request meets the requirement of Article 54 EPC. For similar reasons, the further independent claims directed to a corresponding arrangement (claim 19), and to a mobile terminal (claim 30) and a network node (claim 33) adapted to perform, in cooperation, the method of claim 1, also meet the requirement of Article 54 EPC. The dependent claims, by their reference to the independent claims, are novel too.

6. Main request - inventive step

6.1 Closest prior art

It was common ground in the written and oral submissions of the parties that D4 has to be considered as the prior art closest to the subject-matter of claim 1.

D4 relates to the cryptanalysis of the A5 algorithms used in GSM. D4 states that a vulnerability has been identified for the A5/2 algorithm, which may compromise a mobile station even when subsequently using a different A5 algorithm since distinct A5 algorithms all use the same key generated by the AKA procedure between base and mobile stations. D4 proposes in section 8, "Summary", to cope with this problem by making the keys used in A5/1 and A5/2 unrelated to the keys that are used in A5/3. D4 therefore hints at key separation between the A5 algorithms, A5/3 on one side and A5/1 and A5/2 on the other.

Since D4 relates to the conventional GSM AKA procedure, the difference between the subject-matter of claim 1 and D4 is that the basic security key resulting from a conventional key agreement procedure is modified in dependence on information representative of the security algorithm selected by the network side, i.e the base station.

6.2 D4 and common general knowledge as illustrated by D18

The opponent argued (see statement setting out the grounds of appeal, page 9) that the objective technical problem can be formulated as: "How, in GSM, may the keys used in one basic algorithm (such as A5/2) be made unrelated to the keys that are used in another basic algorithm (such as A5/3)?" According to the opponent, the skilled person is familiar with the use of the A8 algorithm in GSM for generating a session-specific key K_c based on a single shared key K_i. Based on his further knowledge of the principle of separation of keys used for different purposes, as exemplified by section 13.5.1 of D18, the skilled person would directly consider obtaining different keys for the different GSM encryption algorithms by modifying a basic security key using an input indicative of the selected algorithm. The skilled person would in that way arrive at the subject-matter of claim 1 without the exercise of inventive step.

The board is however not convinced by this line of argument. Firstly, as stated by the proprietor, D4 only proposes that the key for A5/3 be unrelated to the keys used for the A5/1 and A5/2 algorithms. Thus considering that D4 suggests a full key separation between all the A5 algorithms is based on hindsight. Therefore the skilled person is directed by D4 to implement a new key generation procedure for the A5/3 algorithm alone but not to modify the conventional key agreement procedure for the other A5 algorithms. Secondly, D18 clearly mentions in section 13.5.1 that the principle of key separation is that keys for different purposes should be cryptographically separated, further citing as example in Remark 13.32 that a key-encryption key should not be used interchangeably as a data encryption key. The skilled person would thus not be incited by D18 to have different encryption keys for the A5 encryption algorithms. Thirdly, the skilled person would get no hint from D4 or D18 to implement the selection of the algorithm on the network side but would rather consider selection at the terminal side, or on both sides, as equal alternatives.

For these reasons the subject-matter of claim 1 involves an inventive step having regard to the disclosure of D4 and the common general knowledge as exemplified by D18.

6.3 D4 and D20

The opponent argued that the skilled person would also find in D20 the solution to the objective technical problem. In its view, the skilled person would implement in the mobile communication network of D4 the teaching of D20 in respect of deriving algorithm-specific keys based on a shared key SK and a unique algorithm identifier in an internet system (see the paragraphs "Key separation" in both sections 2.2 and 4 of D20).

However, as stated in point 6.2 above, the board first disagrees that D4 suggests having different keys for all cryptographic algorithms of the A-family. Therefore the skilled person would not be incited to combine D20 with D4 since D20 envisages modifying a shared key for all encryption algorithms. Further, no selection of a specific encryption algorithm by the network side is disclosed in D20. Moreover, D20 does not relate to mobile networks.

For these reasons the subject-matter of claim 1 involves an inventive step having regard to the disclosure of D4 in combination with D20.

6.4 D4 and D32

The opponent argued that the skilled person would arrive at the subject-matter of claim 1 by combining the teachings of D4 and D32.

However, the board considers this argument to be void since, as stated by the board in point 5.2 above, D32 does not disclose that the algorithm is selected by the network side, i.e. the server, and that the generated encryption key is specific to the selected algorithm.

For these reasons the subject-matter of claim 1 involves an inventive step having regard to the disclosure of D4 in combination with D32.

6.5 D4 and D5

The opponent argued that the subject-matter of claim 1 does not involve an inventive step, having regard to the combination of D4 and D5. However, the opponent acknowledged, both in the statement setting out the grounds of appeal (see section 6.8 and Figure 1) and during the oral proceedings before the board, that D5 did not disclose a modification of a key after it has been generated by a conventional key agreement procedure, as in claim 1, but rather a modification of the key agreement procedure itself which led to the generation of a key which is modified with respect to a key which would have been issued by the conventional key agreement procedure (see in this respect point 5.3 above). Nevertheless, the opponent argued that the skilled person would see no technical difference between the two ways of proceeding, since the generated keys are in both cases dependent on the selected encryption algorithm (see statement setting out the grounds of appeal, point 6.8 on pages 13 and 14).

The board is not convinced by this line of argument. It is clear that a combination of D4 and D5 does not lead to the same sequence of steps as defined in claim 1, the conventional key agreement procedure being kept unamended in claim 1. Further, the solution provided by claim 1 has the advantage that it requires software updates only in the mobile terminal and at the network side, the original key agreement algorithm (e.g. algorithm A8 in GSM) implemented in hardware in both parts remaining the same (see also paragraphs [0016], [0018] and [0022] of the patent).

For these reasons the subject-matter of claim 1 involves an inventive step having regard to the disclosure of D4 in combination with D5.

6.6 The board thus judges that claim 1 according to the main request meets the requirement of Article 56 EPC, having regard to the prior art on file. For similar reasons, the further independent claims directed to a corresponding arrangement (claim 19), and to a mobile terminal (claim 30) and a network node (claim 33) adapted to perform, in cooperation, the method of claim 1, also meet the requirement of Article 56 EPC. The dependent claims, by their reference to the independent claims, meet the requirements of Article 56 EPC too.

7. Main request - sufficiency of disclosure

The opponent argued that the invention does not address all the attacks set out in paragraphs [0003] to [0005] of the patent and thus does not meet the requirements of Article 83 EPC.

The board considers that this allegation does not constitute a substantiated line of argument as to why the skilled person would not be in a position to put the claimed subject-matter into practice. Thus the board does not see any reason to put into question the compliance of the patent with Article 83 EPC.

8. In conclusion, the board judges that the main request (filed as Auxiliary Request 1 during oral proceedings

before the board) meets the requirements of the EPC and that none of the grounds of opposition under Article 100(a) and (b) EPC prejudice the maintenance of the patent on the basis of the main request.

Order

For these reasons it is decided that:

1. The decision under appeal is set aside.
2. The case is remitted to the department of first instance with the order to maintain the patent on the basis of the following documents:
   - claims 1 to 36, filed as Auxiliary Request 1 during oral proceedings before the board,
   - description pages 2 to 12 of the patent specification,
   - figures 1 to 7 of the patent specification.

The Registrar: The Chair:

Beschwerdekammern des Europäischen Patentamts
Boards of Appeal of the European Patent Office
Chambres de recours de l'Office européen des brevets

K. Götz-Wein A. Ritzka

Decision electronically authenticated