BESCHWERDEKAMMERN DES EUROPÄISCHEN PATENTAMTS

BOARDS OF APPEAL OF THE EUROPEAN PATENT OFFICE

CHAMBRES DE RECOURS DE L'OFFICE EUROPEEN DES BREVETS

Internal distribution code:

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

DECISION
of 30 July 2004

Case Number:	T 0726/03 - 3.5.3
Application Number:	01309272.1
Publication Number:	1248483
IPC:	H04Q 7/38
Language of the proceedings:	EN

Title of invention:
System and method for providing secure communications between wireless units using a common key

Applicant:
LUCENT TECHNOLOGIES INC.

Opponent:
-

Headword:
Common key distribution/LUCENT

Relevant legal provisions:
EPC Art. 54(1)

Keyword:
"Novelty - no"

Decisions cited:
-

Catchword:
-

Europäisches Patentamt
European Patent Office
Office européen des brevets

Beschwerdekammern
Boards of Appeal
Chambres de recours

Case Number: T 0726/03 - 3.5.3

DECISION
of the Technical Board of Appeal 3.5.3
of 30 July 2004

Appellant:

LUCENT TECHNOLOGIES INC.
600 Mountain Avenue
Murray Hill
New Jersey 07974-0636 (US)

Representative:

Buckley, Christopher Simon Thirsk
Lucent Technologies NS UK Limited
Intellectual Property Division
5 Mornington Road
Woodford Green
Essex IG8 0TU (GB)

Decision under appeal:

Decision of the Examining Division of the European Patent Office posted 26 February 2003 refusing European application No. 01309272.1 pursuant to Article 97(1) EPC.

Composition of the Board:

Chairman: A. S. Clelland
Members: D. H. Rees
M.-B. Tardo-Dino

Summary of Facts and Submissions

I. This is an appeal from the decision of the examining division to refuse the European patent application number 01 309 272.1, publication number 1 248 483, dispatched on 26 February 2003. The reason given for the decision was that the claimed subject-matter was not novel over the disclosure of

D1: EP-A-0 810 754.

II. Notice of appeal was filed and the fee paid on 11 April 2003. New claims 1 to 3 and 6 to 11 were submitted with a statement setting out the grounds for the appeal on 19 June 2003.

III. In a communication the board gave its preliminary view that the subject-matter of the newly-filed claims still lacked novelty or inventive step with respect to D1 and the general knowledge in the art. The appellant was also asked to clarify the status of claims 4 and 5.

IV. The appellant responded on 14 April 2004 with arguments for the novelty and inventive step of the claimed subject-matter. It was stated that claims 4 and 5 submitted with the letter dated 7 January 2003 were maintained.

V. The appellant requests that the decision of the examining division be cancelled in its entirety and a patent granted on the basis of the following text:

Claims:	1-3,6-11 submitted with the grounds of appeal; 4 and 5 submitted with the letter dated 7 January 2003 and received 9 January 2003.

Description:	pages 2-5,9,11-14,16 as originally filed;
	1,5a,6-8,10,15,17 as received on 25 July 2002 with letter of 22 July 2002;

Drawing:	sheets 1-5 as originally filed.

Claims 1 to 3 read as follows:

"1. A method of providing secure communications between a first wireless unit (70, 80) and a second wireless unit (72, 82), said method being characterized by:
sending a common encryption key (CK_C) to a first wireless unit (70, 80) and second wireless unit (72, 82), for use by said first wireless unit (70, 80) to decrypt information, which has been encrypted at said second wireless unit (72, 82) using said common encryption key (CK_C) and transmitted to said first wireless unit during secure communications over at least one wireless communications system (74, 84, 86) between said first wireless unit (70, 80) and said second wireless unit (72, 82).

"2. The method as claimed in claim 1 wherein said step of sending comprises the steps of:
generating a first key value (CK_1) corresponding to said first wireless unit (70, 80);
generating a common encryption key (CK_C); and

sending said generated common encryption key (CK_C) to said first wireless unit using said first key value (CK_1).

"3. The method as claimed in claim 2 comprising:
generating a second key value (CK_2) corresponding to said second wireless unit (72, 82); and
sending said common encryption key (CK_C) to said second wireless unit using said second key value (CK_2)."

No request for oral proceedings has been made.

Reasons for the Decision

1. The appeal satisfies the requirements of Articles 106 to 108 and Rule 64 EPC and is therefore admissible.

2. In view of the final outcome of the appeal the board has not seen any necessity to investigate whether the amendments made during examination and appeal proceedings satisfy the requirements of Article 123(2) EPC.

3. Interpretation of the claimed subject-matter.
Claim 1 includes the feature "sending a common encryption key (CK_C) to a first wireless unit (70, 80) and second wireless unit (72, 82)." At first sight this might be taken to mean that the same text or string of data is sent to both wireless units. However it is clear that such an interpretation is not in accordance with the description, which specifies that the common encryption key is sent to first and second wireless units in encrypted form, using respective first and

second session key values (as defined in dependent claims 2 and 3). A common encryption key is therefore only sent in the sense that the received key is processed in the wireless units to derive the common encryption key. It is in this sense that the claim is interpreted by the board.

4. D1 discloses:

A method of providing secure communications (column 2, lines 7 to 9) between a first wireless unit (Figure 1, 2a) and a second wireless unit (2b), said method being characterized by:
providing a common encryption key (Kb + RAND + Ka - column 11, lines 3 to 7 and 37 to 49, and see discussion below) to a first wireless unit (2a) and second wireless unit (2b), for use by said first wireless unit (2a) to decrypt information, which has been encrypted at said second wireless unit (2b) using said common encryption key (Kb + RAND + Ka) and transmitted to said first wireless unit during secure communications over at least one wireless communications system (4a, 4b, 6a, 6b, 15) between said first wireless unit (2a) and said second wireless unit (2b) (column 11, line 54, to column 12, line 3).

5. D1 does not refer to "sending a common key value" directly. However, as noted at point 3 above, a common key value is not in fact sent in the preferred embodiment of the application either, but rather a key value which enables the common key to be derived. In D1 the sent keys are described as "partial keys" (e.g. column 11, lines 3 to 7). These partial keys are given by expressions "Kb + RAND" and "Ka + RAND" (where "+"

denotes the exclusive-OR operation). In the terminals these values are exclusive-ORed with Ka and Kb respectively to permit the common key value Ka + RAND + Kb to be derived (column 11, lines 37 to 44). Indeed, the partial keys sent in D1 can be represented mathematically as the common key exclusive-ORed with Ka or Kb, respectively, since (for terminal 2a, for example)

$$\begin{aligned} Kb + RAND &= (Kb + RAND) + 0 \\ &= (Kb + RAND) + (Ka + Ka) \\ &= (Kb + RAND + Ka) + Ka \end{aligned}$$

In other words, what is sent in D1 can be viewed as the common key encrypted (by exclusive-ORing) with a key belonging to the terminal, that is the "common encryption key (CK_C) to said first wireless unit using said first key value (CK_1)," in the terms of claim 2, and therefore also of claim 1.

6. The appellant argues that in D1 the enciphering key itself is never sent between the two units, and that "the enciphering key is calculated at each wireless unit only after corresponding terminal keys are sent from the other wireless unit," (appellant’s response of 14 April 2004). The board notes however that in D1, as in the present application (Claim 1: "sending a common encryption key (CK_C) to a first wireless unit (70, 80) and second wireless unit (72, 82)"), the keys are not communicated from one unit to the other, but rather from a central database station to each of the units (D1, column 11, lines 3 to 7). Hence, the board supposes that what the appellant means by the "corresponding terminal keys" are the keys designated

as "partial keys" in D1, and "between the two units" means "from the central unit to the two units." With this in mind it is clear from the arguments already given that in D1 the enciphering key itself is indeed sent to the two units, in an encrypted form, in the same sense as in the present application.

7. As to when and where the common key is calculated, the appellant’s arguments implicitly assume that claim 1 is limited to providing the same key to all units. As noted above, see point 3, although in the present application a common key may be calculated in the central unit in plaintext, this is not what is sent. The common key is in practice sent in encrypted form, i.e. it is derivable in the wireless units. The fact that in the embodiment the key is calculated centrally in unencrypted form, i.e. in plaintext, is not reflected in the wording of the independent claim, and is therefore not relevant to the question of its novelty.

8. Finally the appellant argues that D1 does not explicitly teach that what is sent is an encrypted form of the common key. This is, however, not relevant to the question of novelty, since the method specified in claim 1 of the present application is nonetheless directly and unambiguously derivable from the disclosure of D1.

9. Hence the subject-matter of claim 1 is known from the disclosure of D1, and the text of the appellant’s sole request does not satisfy the requirements of Articles 52 and 54 EPC. There being no other requests, it follows that the appeal must be dismissed.

Order

For these reasons, it is decided that:

The appeal is dismissed.

The Registrar: The Chairman:

D. Magliano A.S. Clelland