**BESCHWERDEKAMMERN<br>DES EUROPÄISCHEN<br>PATENTAMTS**

**BOARDS OF APPEAL OF<br>THE EUROPEAN PATENT<br>OFFICE**

**CHAMBRES DE RECOURS<br>DE L'OFFICE EUROPÉEN<br>DES BREVETS**

**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 July 2021

**Case Number:** T 0995/17 - 3.5.03

**Application Number:** 02767632.9

**Publication Number:** 1428403

**IPC:** H04W12/02

**Language of the proceedings:** EN

**Title of invention:**
Communications methods, systems and terminals

**Patent Proprietor:**
Motorola Solutions, Inc.

**Opponent:**
SEPURA LIMITED

**Headword:**
Secure group communications/MOTOROLA

**Relevant legal provisions:**
EPC Art. 56
RPBA Art. 12(4)

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

**Keyword:**

Admittance of late-filed documents - (no): could have been filed earlier and no prima facie relevance
Inventive step - (yes)

Europäisches Patentamt
European Patent Office
Office européen des brevets

**Beschwerdekammern**

**Boards of Appeal**

**Chambres de recours**

Boards of Appeal of the
European Patent Office
Richard-Reitzner-Allee 8
85540 Haar
GERMANY
Tel. +49 (0)89 2399-0
Fax +49 (0)89 2399-4465

**Case Number: T 0995/17 - 3.5.03**

# DECISION
## of Technical Board of Appeal 3.5.03
## of 21 July 2021

**Appellant:**
(Opponent)

SEPURA LIMITED
9000 Cambridge Research Park
Beach Drive
Waterbeach
Cambridge CB25 9TL (GB)

**Representative:**

Dehns
St. Bride's House
10 Salisbury Square
London EC4Y 8JD (GB)

**Respondent:**
(Patent Proprietor)

Motorola Solutions, Inc.
1303 East Algonquin Road
Schaumburg IL 60196 (US)

**Representative:**

Wray, Antony John
Optimus Patents Limited
Peak Hill House
Steventon
Basingstoke, Hampshire RG25 3AZ (GB)

**Decision under appeal:**

**Decision of the Opposition Division of the European Patent Office posted on 10 February 2017 rejecting the opposition filed against European patent No. 1428403 pursuant to Article 101(2) EPC.**

**Composition of the Board:**

| | |
|---|---|
| **Chair** | K. Bengi-Akyürek |
| **Members:** | K. Schenkel |
| | N. Obrovski |

## Summary of Facts and Submissions

I. The appeal of the opponent (appellant) lies from the decision of the Opposition Division rejecting the opposition filed against the present European patent *inter alia* on the ground that the subject-matter of claims 1 and 8 as granted involves an inventive step (Article 56 EPC), having regard to the disclosure of

**D1**: US 5 357 571;<br>
**D8**: Bluetooth v1.0 B, 1 December 1999; "Specification of the Bluetooth System: Wireless connections made easy", pp. 41-169;<br>
**D9**: IEEE Std 802-1990, December 31, 1990; "IEEE Standards for Local and Metropolitan Area Networks: Overview and Architecture", pp. 1-31.

II. Oral proceedings before the board were held on 21 July 2021 by videoconference in accordance with the appellant's request. The respondent did not attend those oral proceedings as announced.

- The appellant requested that the decision under appeal be set aside and that the patent be revoked.

- The respondent had requested in writing that the appeal be dismissed and that the patent be maintained as granted (**main request**) or, in the alternative, that the patent be maintained on the basis of a **first** or a **second auxiliary request**, both filed with the reply to the appellant's statement of grounds of appeal.

At the end of the oral proceedings, the board's decision was announced.

III. Claim 1 of the **main request** reads as follows:

"A method of providing secure group communications in a communication system (100) between a plurality of terminals (112, 114, 116) employing an encryption protocol that uses a shared encryption key in each of the plurality of terminals in the group, the method including modifying a shared encryption key associated with the group in a transmitting terminal (112) to provide a modified encryption key and encrypting information to be transmitted by the transmitting terminal using the modified encryption key, wherein the shared encryption key is modified by combining the shared encryption key with an identifier (520) providing a unique identification of the transmitting terminal, characterised in that:

(i) the identifier (520) is a Medium Access Control (MAC) address given to the transmitting terminal (112); and

(ii) the identifier (520) is transmitted in control signalling by the transmitting terminal (112) by wireless communication to a plurality of receiving terminals (114, 116), and is extracted and recognised by the plurality of receiving terminals (114, 116)."

## Reasons for the Decision

1. *Background of the opposed patent*

The present patent relates to the technical field of secure communications between terminals of a group, reference being made to private communication systems operating according to the TETRA standard, as used for example by fire or police forces or within companies. In such systems, security is mainly achieved by means of key-based encryption which however gives rise to several challenges. To enable private communications between two terminals which is not intelligible by others of the group, for example, a different key or key pair would be necessary for each conceivable combination of users, which constitutes a large key management problem (see paragraph [0015] of the patent specification).

In order to address this challenge, the patent proposes that a shared encryption key is associated to the group and is modified by the transmitting terminal by combining it with a "unique identifier" of the transmitting terminal. A shared key is defined in the patent as an identical encryption key which is used by both the sender and the recipient (paragraph [0009]). More specifically, the unique identifier is a "Medium Access Control (MAC) address" of the transmitting terminal and is transmitted by means of "control signalling" by the transmitting terminal.

## *2. Main request - inventive step (Article 56 EPC)*

First, it is noted that the board construes the term "group communications" according to present claim 1 broadly, i.e. as referring to any type of communication between members of a group of communication terminals.

### 2.1 Prior-art document **D1**

2.1.1 The document relates also to the field of secure communications among communication units of a group and likewise mentions the challenge relating to secure a communication between two members of the group with respect to the other group members. In particular, it proposes a communication system providing secure point-to-point (P2P) communication between communication units, each communication unit storing a set of encryption key variables (column 2, lines 27 to 31).

A first (transmitting) communication unit (terminal) generates a "private call key variable" (corresponding to the *modified encryption key* as claimed) by modifying an "encryption key variable" (corresponding to the *shared encryption key* as claimed) using a "predetermined function" (column 2, lines 35 to 38). The first communication unit transmits information related to the *encryption key variable* and the predetermined function to a destination communication unit which generates the *private call key variable* based on the received information (column 2, lines 38 to 45). The first communication unit and the destination communication unit can then start a secured private call using the *private call key variable* (column 2, lines 45 to 51 and column 5, lines 60 to 63).

2.1.2 In a *first example,* the predetermined function is based on a user code which is entered by the user of the first communication unit and the user of the destination communication unit (column 4, lines 6 to 10; column 5, lines 16 to 19, and 36 to 41). In a *second example*, the predetermined function is based on an identification code of the first or of the destination communication unit or on a combination of both (column 4, lines 15 to 22).

2.1.3 In order to provide the destination communication unit with the *private call key variable* or, in other words, to enable the destination communication unit to generate the *private call key variable*, two approaches A and B are disclosed (column 4, lines 60 to 63).

2.1.4 In approach A, an identification of the *encryption key variable*, based on which the *private call key variable* has been generated, and information pertaining to the predetermined function is transmitted to the destination communication unit (column 4, line 66 to column 5, line 2). However, **D1** does not provide further details about the transmission to the destination communication unit.

2.1.5 In approach B, which is used only for the *second example* of the predetermined function, the first communication unit generates an encrypted message using the *private call key* and transmits it to all communication units together with the *encryption key variable*, which has been used to generate the *private call key*, but without the unique identification code of the first and/or destination communication unit (column 6, lines 2 to 23). Thus, all communication units which receive the encrypted message try to generate the private call key but only the destination communication communication unit will successfully generate the correct private call key (column 6, lines 28 to 31 and 35 to 38).

2.2 The board, in line with the appellant's arguments, considers the method of **D1**, which uses the predetermined function according to the *second example* and approach A, to be the most promising starting point for assessing the question of inventive step.

In view of the above, the method of claim 1 differs from this method in that

(a) the identifier used for modifying the shared encryption key is a MAC address (i.e. feature (i) as claimed) and
(b) the identifier is transmitted in control signalling (i.e. feature (ii) as claimed).

2.3 As to distinguishing feature (a), the MAC address is a unique identifier used as a terminal address at the second (i.e. data-link) layer of the well-known seven-layer OSI model for transferring data between different network segments (links). The technical effect of feature (a) is hence that a single identifier is used for both data-link transmissions and for providing the secure group communications, whilst transmitting the MAC address in control signalling separately from the user data channels according to distinguishing feature (b) increases the overall data security.

2.4 Starting out from the method of **D1**, the objective technical problem underlying the claimed subject-matter may therefore be seen in "providing secure group communications while ensuring a lean data overhead".

2.5 Considering that usually the MAC address is not transmitted to the recipient terminal (e.g. to avoid the risk of eavesdropping) and that control signalling is not used for transmitting user information, the board concludes that **D1** does not provide any hints towards the aforementioned features (a) and (b).

2.6 The appellant argued that the MAC address uniquely identifies a network device and therefore fulfils all requirements of the unique identification code in the method of **D1**. The skilled person would therefore have considered using the MAC address as identifier providing a unique identification within the meaning of present claim 1.

The board however considers that a MAC address is a very specific identifier for transferring data between network links in the underlying network. In this context, it is typically not transmitted to the final recipient. Hence, the skilled person would not have envisaged the transmission of a source terminal's MAC address to the destination terminal and its use for creating the "private call key".

2.7 The appellant further argued that the transmission of the unique identification code via control signalling was a well-known measure to transmit signals to the destination communication unit.

The board however notes that the appellant did not provide any document in support of this argument and that the control signalling or, in other words, the control plane is commonly used for controlling the network and the transmissions via control (signalling) channels and is kept separate from the data channels to be transmitted between the network terminals.

2.8 In summary, there is no hint in D1 towards the use of a very specific unique identification code, namely the MAC address of a transmitting terminal for the respective key generation, towards transmitting that MAC address to the respective receiving terminals, and towards performing that transmission by means of control signalling to the receiving terminals. The board therefore concludes that the method of claim 1 as granted involves an inventive step having regard to **D1** (Articles 52(1) and 56 EPC).

3. Other independent claims

The above conclusions apply, *mutatis mutandis*, to present system **claim 23** and device **claim 30**.

4. Admittance - documents **D8** and **D9** (Article 12(4) RPBA 2007)

4.1 None of documents D8 and D9 were submitted during the opposition proceedings, although they could have been presented there, as argued by the respondent. Therefore, their admittance is at the discretion of the board (Article 12(4) RPBA 2007).

4.2 Since claim 1 as granted was maintained without changes, these documents should have been submitted during the opposition proceedings in order to raise an inventive-step objection against claim 1 of the main request already at that stage. The appellant refers in this regard to the opposition division's position on the disclosure of **D1** in the decision under appeal. However, the mere fact that the appellant's objection based on D1 did not succeed in the opposition proceedings does not justify the late filing of **D8** and **D9** only in these appeal proceedings.

4.3 As to their substance, **D8** discloses distributing the same information to several recipients using a "common encryption key" in a point-to-multipoint configuration (see page 151, section 14.2.1, fourth paragraph). In this point-to-multipoint configuration, a common key $K_{master}$ is used (page 157, section 14.2.2.6, first paragraph). The generation of $K_{master}$ as described in section 14.2.2.8 on pages 158 and 159, however, does not involve modifying a "shared encryption key" used in each of the plurality of terminals as stipulated by claim 1.

The appellant argued that, based on $K_{master}$, a modified key $K_C$ may be generated (page 159, first paragraph). However, even assuming that key $K_C$ is a modified key used in a point-to-multipoint configuration, it is generated by modifying $K_{master}$, which has been generated only by the members of a broadcast subgroup of terminals within the group, and not by modifying an encryption key shared by all terminals of the group as stipulated by claim 1. Further, in **D8** the modified key $K_C$ is computed by each terminal (cf. page 159, first paragraph).

4.4 In conclusion, **D8** relates to a "Bluetooth system" with standard low-cost devices which can easily and flexibly be paired in any combination. These features distinguish a Bluetooth system fundamentally from a "group communication system" in which first all members of a group are provided with a "shared encryption key" (for secured communication within the whole group), which then is modified for secure communications between a transmitting terminal and a plurality of receiving terminals.

4.5 Hence, the board concludes that **D8** (and **D9** which was introduced to set out the "MAC standard") are *prima facie* not a more promising starting point than D1 for assessing inventive step of claim 1 as granted and are consequently not *prima facie* highly relevant.

4.6 The board therefore did not admit **D8** and **D9** into the appeal proceedings (Article 12(4) RPBA 2007).

5. It follows from the above that the ground for opposition pursuant to Article 100(a) EPC does not prejudice the maintenance of the patent as granted. Other grounds for opposition were not raised during the appeal proceedings. Consequently, the present appeal is to be dismissed.

## Order

### For these reasons it is decided that:

The appeal is dismissed.

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

S. Lichtenvort K. Bengi-Akyürek

Decision electronically authenticated