Internal distribution code:

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

Datasheet for the decision of 16 September 2024

Case Number: T 2551/22 - 3.5.05

Application Number: 14197825.4

Publication Number: 3032858

IPC: H04W12/04, H04R25/00, H04L9/08, H04L29/06, H04L9/14

Language of the proceedings: EN

Title of invention:
Apparatus for secure hearing device communication and related method

Patent Proprietor:
GN Hearing A/S

Opponent:
Oticon A/S

Headword:
Session key for hearing aids/GN HEARING

Relevant legal provisions:
EPC Art. 56
RPBA 2020 Art. 12(4)

Keyword:

Inventive step - main request (no)
Admittance of claim amendments filed on appeal - auxiliary requests (no): not suitable to address the relevant issues

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

Case Number: T 2551/22 - 3.5.05

D E C I S I O N
of Technical Board of Appeal 3.5.05
of 16 September 2024

Appellant: (Opponent)	Oticon A/S Kongebakken 9 2765 Smørum (DK)
Representative:	Cohausz & Florack Patent- & Rechtsanwälte Partnerschaftsgesellschaft mbB Bleichstraße 14 40211 Düsseldorf (DE)
Respondent: (Patent Proprietor)	GN Hearing A/S Lautrupbjerg 7 2750 Ballerup (DK)
Representative:	Aera A/S Niels Hemmingsens Gade 10, 5th Floor 1153 Copenhagen K (DK)
Decision under appeal:	**Interlocutory decision of the Opposition Division of the European Patent Office posted on 26 September 2022 concerning maintenance of the European Patent No. 3032858 in amended form.**

Composition of the Board:

Chair	K. Bengi-Akyürek
Members:	P. Tabery
	C. Heath

Summary of Facts and Submissions

I. The appeal is directed against the opposition division's decision to maintain the present patent in amended form according to an "auxiliary request".

II. The opposition division found that the claims as granted contained added subject-matter (Article 100(c) EPC).

III. The prior-art documents referred to by the opposition division included:

D1: US 2012/0140962 A1
D2: US 8,745,394 B1.

IV. Oral proceedings before the board were held on 16 September 2024.

The final requests of the appellant-opponent (henceforth "the opponent") were that the decision under appeal be set aside and that the patent be revoked.

The final requests of the respondent-proprietor (henceforth "the proprietor") were that the appeal be dismissed (**main request**), or that the patent be maintained on the basis of one of **auxiliary requests C1 to C4** filed with the written reply to the statement of grounds of appeal.

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

V. Claim 1 of the **main request** reads as follows (board's labelling):

F1 "A client device (110) for hearing device communication, the client device (110) comprising
F1.1 a processing unit (202);
F1.2 a memory unit (203); and
F1.3 an interface (204),
wherein the processing unit (202) is configured to:
F1.4 send a session request (301) for a session to the hearing device via the interface (204);
F1.5 receive a session response (302) from the hearing device via the interface (204),
F1.5.1 the session response (302) comprising a hearing device identifier;
F1.6 obtain a session key based on the session response (302), wherein to obtain a session key comprises
F1.6.1 to establish a connection to a session key device (111) via the interface (204),
F1.6.2 to send a session key request (304) to the session key device (110) via the interface (204),
M1.6.2.1 the session key request (304) comprising the hearing device identifier,
F1.6.3 to receive a session key response (305) from the session key device (110) via the interface (204),
F1.6.4 to determine the session key based on the session key response (305);
F1.7 determine hearing device data;
F1.8 generate session data (303) based on the session key and the hearing device data; and

F1.9 send the session data (303) to the hearing device via the interface (204)."

Claim 1 of **auxiliary request C1** differs from claim 1 of the main request in that the following wording has been inserted between features F1.6.1 and F1.6.2:

F2 ", wherein the connection to the session key device (111) is a secure connection over a network".

Claim 1 of **auxiliary request C2** differs from claim 1 of auxiliary request C1 in that the phrase "and an encrypted session key" has been added at the end of feature F1.5, and in that the following wording has been inserted between features F1.6.4 and F1.7:

F5 ", wherein to determine the session key comprises retrieving the session key from the session key response (305)," and

F6 "retrieving a hearing device key from the session key response (305), and decrypting the encrypted session key based on the hearing device key".

Claim 1 of **auxiliary request C3** differs from claim 1 of auxiliary request C2 in that the following wording has been added between features F1.8 and F1.9:

F7 ", wherein to generate the session data (303) based on the session key and the hearing device data comprises generating a message authentication code based on the session key and the hearing device data;" and

F8 "or digitally signing the hearing device data".

Claim 1 of **auxiliary request C4** differs from claim 1 of auxiliary request C3 in that the following phrase has been added at the end of feature F1.7:

F9 ", wherein the hearing device data comprises firmware".

Reasons for the Decision

1. The opposed patent concerns the communication of a hearing aid device with a client device which permits remote fitting of the hearing aid device. The communication is secured by means of a session key, which is established during session setup.

2. Main request

2.1 Inventive step (Article 56 EPC)

2.1.1 Although not disclosed in document D1, the board holds that features F1.5, F1.5.1 and F1.6.3 cannot distinguish the claimed apparatus from the prior art, since they are merely defining the apparatus by the contents of messages which are to be *received*. However, a receiver has no control over the contents of the messages it receives. Nevertheless, in the proprietor's favour, these features will be regarded in the following as being limiting and distinguishing features.

2.1.2 It follows from the above that the subject-matter of claim 1 differs from the disclosure of document **D1** in

features F1.5.1 to F1.6.4, F1.8 and F1.9. As to features F1.8 and F1.9, it is noted that it is only the aspect how the "session key" is *retrieved* which is not disclosed. In view of the breadth of the term "session key", an "encryption key" as implicitly disclosed in paragraph [0140] of document D1 can well be read onto it.

2.1.3 The board is not convinced by the proprietor's argument that, additionally, document D1 did not disclose **features F1.4** and **F1.5** relating to a "session request" and "session response", since paragraph [0141] of D1 did not even mention the term "session". Rather, as argued by the opponent, this paragraph of D1 in fact discloses an access operation to edit data using a wireless or wirebound communication protocol and thus necessarily involves a "communication session" as a time-limited network connection. Therefore, the board holds that features F1.4 and F1.5 are implicitly disclosed by document D1.

2.1.4 Moreover, the board is not convinced by the proprietor's argument that document D1 did not disclose that the "operability data" (denoted "hearing device data" in claim 1) were generated by the fitting apparatus and that thus **feature F1.7** also constituted a distinguishing feature. As argued by the opponent, paragraph [0142] of document D1 in fact discloses that "a data set 12 will be created and stored in a storage unit 10 of fitting apparatus 7 when operability data 5 are edited, wherein data set 12 reflects the new/edited operability data 5". The board understands that, in the system of D1, the "data set 12" comprises information which is effectively identical to the "operability data 5" and that the claimed "session data" is

anticipated by what is transmitted in D1 to cause that the hearing device's "operability data 5 are edited".

2.1.5 The board cannot accept the technical effect invoked by the proprietor that an "improved secure communication" would be provided, including "secure and/or authorized access to the memory of the hearing device". Notably, the proprietor did not indicate which specific aspect of the secure communication would actually be improved. Hence, it cannot be objectively verified whether the distinguishing features actually achieve an improvement. Claim 1 does not deal with authorisation and thus the distinguishing features may not provide an improvement relating to an "authorised access". Moreover, the board does not subscribe to the proprietor's argument that secure access to the memory of the hearing device would be enabled. Instead, claim 1 is only related to the "client device" and thus does not include specific features of the "hearing device".

2.1.6 Rather, the board concurs with the opponent that the distinguishing features achieve the technical effect of implementing the encrypted communication between the hearing device 2 and the external fitting apparatus 7 of document D1.

2.1.7 The objective technical problem may thus be formulated as "how to implement the encrypted communication between the hearing device 2 and the external fitting apparatus 7 of document D1".

2.1.8 As submitted by the opponent, document **D2** teaches in column 5, lines 58-63 that key pairs may be stored in a "hardware security module". Evidently, the use of such a "module" indeed implies the steps of **features F1.6 to**

F1.6.3 relating to retrieving a public/private key pair ("session key response" in claim 1) from the "hardware security module" ("session key device" in claim 1).

2.1.9 Moreover, document D2 discloses in column 6, lines 36-46 that the "session key" is decrypted using the obtained private key. Thus, distinguishing **feature F1.6.4** is likewise disclosed. For the sake of completeness, it is noted that such a step is even unnecessary in case the session key is an *asymmetric* key (as implied in dependent claim 8), since the obtained private key may already serve as the "session key". The security keys being identical, **feature F1.6.4** is merely tautological in that case.

2.1.10 Last but not least, distinguishing **features F1.5.1** (receiving a device ID) as well as **features F1.8 and F1.9** (use of the "session key" for encryption) follow necessarily from **features F1.6 to F1.6.3**: To retrieve a public/private key pair, it needs to be identified; it is the very purpose of "session keys" to be used within a "session".

2.1.11 Hence, when combining the teaching of document D1 with the above teachings of document D2, the skilled person would have readily arrived at the subject-matter of claim 1 without employing any inventive skill.

2.1.12 In that regard, the board concurs with the opponent that the skilled person would have been capable and motivated to extract the concept of using a "hardware security module" for public/private key pairs from another document. In particular, it is immediately apparent that the "hardware security module" is not intrinsically linked with being used by a *server* and a *client* communicating with the server. Likewise, the

concept of decrypting a received message using the private key is independent of being performed by a server. Therefore, the board holds that the skilled person would have readily combined the relevant teachings of documents **D1** and **D2**, depending on the required level of security.

2.1.13 The board does not subscribe to the proprietor's argument that the skilled person would not have considered combining the teachings of document D1 and D2, as the latter mentioned a "public key of ... a financial institution" and was thus related to the field of financial security. Rather, the board considers that document D2 belongs to the field of "secure communication" (see abstract of document D2) and thus indeed from a neighbouring field. Since document D2 mentions the "financial institution" only as a possible application of the mechanisms described therein, it is apparent to the skilled person that D2 provides a teaching which is applicable wherever "secure communication" at the respective level is required.

2.1.14 In this context, the board concurs with the opponent that the skilled person cannot be limited to being knowledgeable either in the field of hearing aids or in the field of communication security. Rather, since cryptography is increasingly important for hearing aids, the person skilled in the field of hearing aids would consult the person skilled in secure communications.

2.1.15 In addition, the board does not subscribe to the proprietor's argument that the claimed solution involved an inventive step, since there would be too many possible options to solve the objective technical

problem. Since claim 1 does not specify any particular security mechanism, it is immaterial which of the many available security mechanisms the skilled person would have ultimately selected, as he would have arrived at an embodiment falling well within the claimed subject-matter anyhow.

2.1.16 Moreover, the board is not persuaded by the proprietor's argument that feature F1.6.2 was not obvious, as it specifies that the "session key request" is sent to the "session key device" via the same interface as the "session request" to the "hearing device". Rather, the skilled person would have envisaged sending the latter via a short-range wireless interface (e.g. Bluetooth) and the former via a WLAN interface (i.e., what is typically used for Internet access). Since the term "interface" is left undefined in claim 1, it also comprises purely internal hardware interfaces as well as any type of software interfaces. It would have been commonly known to the skilled person at the relevant date that such interfaces are necessarily used when the combined teaching of document D1 and D2 is put into practice.

2.1.17 Finally, the board is not convinced by the proprietor's argument that a "backend server" could not "reasonably be seen as a hearing device". According to the opponent's and the opposition division's line of argumentation, the "backend server" of D2 is mapped to the "fitting device" of D1.

2.1.18 Consequently, the subject-matter of claim 1 of the main request is not inventive over the disclosure of document **D1** in combination with the relevant teaching of document **D2**.

2.2 In view of the above, the main request is not allowable under Article 56 EPC.

3. Admittance of auxiliary requests (Article 12 RPBA)

3.1 **Auxiliary requests C1 to C4** are amended claim requests which were not presented in the opposition proceedings. Their admittance into these appeal proceedings is therefore governed by the relevant parts of Article 12 RPBA. One of the criteria mentioned in Article 12(4), fifth sentence, RPBA is the suitability of the amendment to address the issues which led to the decision under appeal.

3.2 The board does not subscribe to the proprietor's argument that the auxiliary requests were filed in reaction to the generalisation of the teaching of document D2, as this had been mentioned for the first time in the decision under appeal. Although the opposition division had not agreed with this line of attack, on an objective basis, it constituted a reason for filing new amendments at that late stage of the proceedings. Rather, the board concurs with the opponent that this generalisation was not a new position, but was already presented with the notice of opposition. Therefore, this does not constitute a reason for submitting these amendments only in the appeal proceedings.

3.3 As to **auxiliary request C1**, the board is not convinced by the proprietor's argument that **feature F2** enhanced the effect to allow for secure access to the memory of the hearing device. If at all, this effect is already achieved by the other features of claim 1. Rather, feature F2 allows for connecting to remote session key devices, where the fact that the session key device is

remote may be a requirement set by the manufacturer. The board holds that using secure network connections to communicate with distant entities was commonly known to the skilled person at the patent's filing date and may thus not contribute to an inventive step. Therefore, the amendment (feature F2) is not suitable to address the objection as to lack of inventive step.

3.4 With respect to **auxiliary request C2**, the board concurs with the opponent that **features F5 and F6** were already considered in the context of the main request as being known from document D2. Therefore, the amendment (features F5 and F6) is not suitable to address the objection as to lack of inventive step.

3.5 Having regard to **auxiliary request C3**, the board concurs with the opponent that **features F7** and **F8** constitute measures which were commonly known at the patent's filing date for securing data connections. The board adds that feature F7 was known to ensure integrity of messages, while feature F8 was known to ensure non-repudiation at the relevant date. Therefore, the amendment (features F7 and F8) is not suitable to address the objection as to lack of inventive step.

3.6 Finally, claim 1 of **auxiliary request C4** defines in **feature F9** merely that "firmware" is transmitted, i.e. just another item is sent. However, data transmission as such constitutes a measure which was commonly known at the patent's filing date and may thus not contribute to an inventive step. Therefore, the amendment (feature F9) is not suitable to address the objection as to lack of inventive step.

3.7 In view of the above, the board holds that none of the amendments is suitable to address the issues which led

to the decision under appeal. Therefore, the board exercised its discretion not to admit auxiliary requests C1 to C4 into the appeal proceedings (Article 12(4), fifth sentence, RPBA).

Order

For these reasons it is decided that:

1. The decision under appeal is set aside.

2. The patent is revoked.

The Registrar: The Chair:

B. Brückner K. Bengi-Akyürek

Decision electronically authenticated