Internal distribution code:

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

Datasheet for the decision of 13 November 2024

Case Number: T 0487/22 - 3.5.05

Application Number: 14197823.9

Publication Number: 3032857

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

Language of the proceedings: EN

Title of invention:
Hearing device with communication protection and related method

Patent Proprietor:
GN Hearing A/S

Opponent:
Oticon A/S

Headword:
Secure communication in a hearing aid/GN HEARING

Relevant legal provisions:
EPC Art. 56, 100(a)

Keyword:
Inventive step - all claim requests (no): correct application of the "partial-problem" approach

Decisions cited:
T 1019/99

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 0487/22 - 3.5.05

D E C I S I O N
of Technical Board of Appeal 3.5.05
of 13 November 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:	**Decision of the Opposition Division of the European Patent Office posted on 17 December 2021 rejecting the opposition filed against European patent No. 3032857 pursuant to Article 101(2) EPC.**

Composition of the Board:

Chair	K. Bengi-Akyürek
Members:	K. Peirs
	F. Bostedt

Summary of Facts and Submissions

I. The appeal lies from the decision of the opposition division to reject the opposition (Article 101(2) EPC). The opposition division considered that the ground for opposition under Article 100(a) EPC in conjunction with Articles 54 and 56 EPC did not prejudice the maintenance of the opposed patent in its granted form.

In the appealed decision, the opposition division took into account the following prior-art document:

D1: US 2012/0140962 A1.

II. Oral proceedings before the board were held on 13 November 2024. The parties' final requests were as follows:

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

- The respondent requested that the appeal be dismissed (**main request**). In the alternative, it requested that the patent be maintained in amended form on the basis of one of five auxiliary requests (**auxiliary requests 1 to 5**).

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

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

(a) "A hearing device (101) comprising

(b) - a processing unit (202) configured to compensate for hearing loss of a user of the hearing device;
(c) - a memory unit (203); and
(d) - an interface (204),
characterized in that
(e) the processing unit (202) is configured to:
- receive a session request (301) for a session via the interface (204);
(f) - obtain and store a session key;
(g) - encrypt the session key based on a hearing device key,
(h) wherein the hearing device key is stored in a permanent memory of the hearing device (101);
(i) - send a session response (302) comprising the encrypted session key; and
(j) - receive session data (303) in the session via the interface (204)."

IV. Claim 1 of **auxiliary request 1** differs from claim 1 of the main request in that feature (h) is replaced by the following feature (board's feature labelling and underlining, the latter reflecting amendments vis-à-vis feature (h)):

(k) "wherein the hearing device key is a symmetric key and stored in a permanent memory of the hearing device (101);".

V. Claim 1 of **auxiliary request 2** differs from claim 1 of auxiliary request 1 in that feature (i) is replaced by the following feature (board's feature labelling and underlining, the latter reflecting amendments vis-à-vis feature (i)):

(l) "- send a session response (302) comprising the

encrypted session key and a hearing device identifier; and".

VI. Claim 1 of **auxiliary request 3** differs from claim 1 of auxiliary request 2 in that it comprises, at the end, the following feature (board's feature labelling):

(m) ";
- decrypt the session data (303) with the session key; and
- store at least part of decrypted session data in the memory unit (203)".

VII. Claim 1 of **auxiliary request 4** differs from claim 1 of auxiliary request 3 in that the word "and" is deleted at the end of feature (l) and in that feature (j) is replaced by the following feature (board's feature labelling and underlining, the latter reflecting amendments vis-à-vis feature (j)):

(n) "- receive session data (303) in the session via the interface (204)), the session data (303) comprising fitting data, hearing device operating parameters, and/or firmware data;".

VIII. Claim 1 of **auxiliary request 5** differs from claim 1 of auxiliary request 4 in that it comprises, at the end, the following feature (board's feature labelling):

(o) ", wherein the processing unit (202) is configured to compensate for hearing loss of a user of the hearing aid according to the received session data (303)".

Reasons for the Decision

1. *Technical background*

1.1 The opposed patent addresses the problem of securing the data communication between a hearing device and external devices, such as smartphones, tablets or fitting devices, to prevent unauthorised access and potential risks like malfunction or battery drain.

1.2 Figure 2 of the opposed patent illustrates a hearing device with the claimed security features.

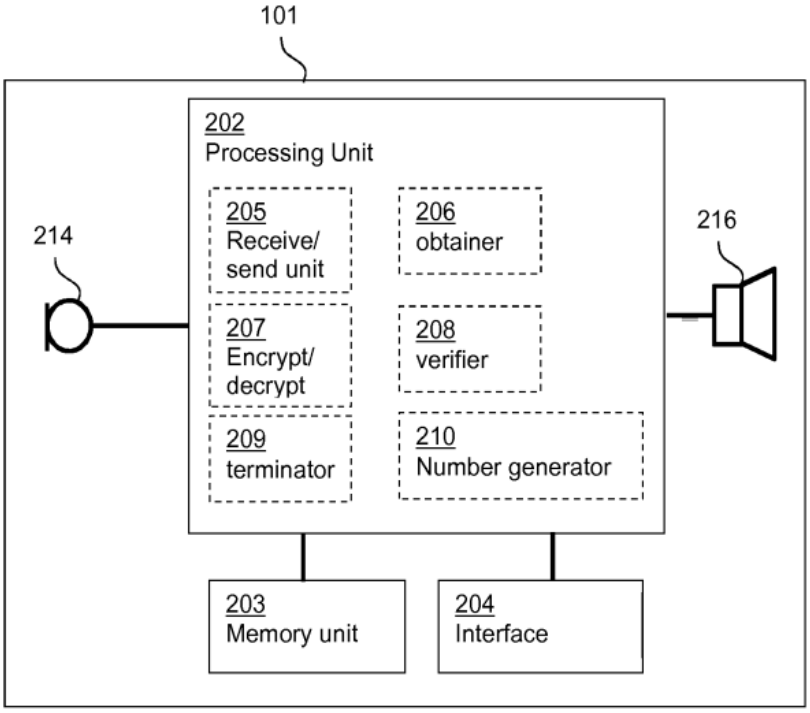

Fig. 2

Processing unit 202 is configured to compensate for a user's hearing loss. It is also responsible for receiving (205) a session request, obtaining (206), storing (203) and encrypting (207) a session key and

sending (205) a session response. It further decrypts (207) received session data and verifies (208) the integrity of this received session data.

1.3 By using a unique session key for each communication session and encrypting it with a so-called "hearing-device key" stored securely in the hearing device's memory, the patent's solution is supposed to ensure that only authorised devices with the correct hearing-device key can establish a secure connection and exchange data with the hearing device. The integrity verification of session data is said to prevent unauthorised modification or tampering, further enhancing security.

2. *Main request: claim 1 - construction*

2.1 The term "session key" as mentioned in claim 1 as granted typically refers to a (single-use) symmetric key used for encrypting all data messages in one communication session. In other words, the term "session key" implies the use of one key only, which is typically solely the case in *symmetric* encryption schemes. By contrast, *asymmetric* encryption schemes are normally characterised by two different keys, namely a "public" and a "private" one.

2.2 Regarding **feature (g)**, the appellant argued that the hearing-device key "is used for encrypting the session key".

However, in the board's view, feature (g) is phrased more generally, stating that the "session key" is encrypted *based on* a "hearing device key". This encompasses the realistic case that the encryption key could be retrieved, for instance, via a look-up table

using the "hearing device key". The respondent stated that a hearing-device key was a cryptographic key and that the "skilled person would NEVER use a cryptographic key as an index for a look up table" (capital letters as in the original). However, the respondent did not provide arguments in this regard. The board notes that claim 1 as granted does not explicitly define the "hearing device key" as a cryptographic key or limit it to a specific form. This allows for broader, technically meaningful interpretations, not necessarily limited to just traditional cryptography. The board considers in particular that several pieces of data can indeed fulfil the functionality of encrypting the "session key" in accordance with feature (g).

3. *Main request: claim 1 - inventive step*

The parties agree that document **D1** is the most suitable starting point for the assessment of inventive step. The board sees no reason to dispute this.

3.1 In Reasons C1.1 of the appealed decision, the opposition division found D1 not to disclose features F1.4 to F1.7, i.e. **features (e) to (i)** in the board's labelling. According to Reasons C1.1 of the decision, D1 did not directly and unambiguously disclose that "the same processing unit compensating for hearing loss also performs the session and key exchange steps" (emphasis as in the original). The parties agreed that at least features (f) to (i) were not disclosed in D1. In addition, the respondent considered also features (b), (e) and (j) to constitute distinguishing features.

The board's analysis in this respect is as follows.

3.1.1 "Hearing device 2" (i.e. **feature (a)**) shown in Figure 1 and described in paragraph [0135] of D1 comprises signal processing unit 14, which performs sound processing in dependence of sound processing parameters. These parameters are adjustable to "the hearing needs and preferences of the hearing device user" (emphasis added). The skilled reader would directly and unambiguously understand from this that signal processing unit 14 is a "processing unit" in accordance with **feature (b)**. Moreover, storage unit 16 shown in Figure 1 of D1 stores those parameters and can be seen as the "memory unit" referred to in **feature (c)**. The data exchanges shown in Figure 1 of D1, such as those indicated with arrows 30 and 31, imply an "interface" according to **feature (d)**. According to paragraph [0136] of D1, hearing device 2 comprises non-volatile storage unit 4, which can thus be read onto the "permanent memory" mentioned in **feature (h)**.

The respondent contested that D1 disclosed feature (b), even when considering paragraphs [0134] to [0136] of D1, but the board holds the last sentence of paragraph [0135] of D1 to be unequivocal in this respect.

3.1.2 As regards **feature (e)**, paragraph [0140] of D1 describes fitting apparatus 7 shown in Figure 1 of D1, which has fitting software 9 used for adjusting hearing device 2 "to the hearing needs and preferences of the hearing device user". This adjusting step is typically referred to as "hearing-aid fitting". The respondent correctly stated that such a hearing-aid fitting normally starts with entering the hearing aid into a

"programming mode" by pressing a button. However, once the hearing aid is in such a programming mode, it is usually up to the fitting apparatus to request a connection with the hearing aid to transfer the programming data, as convincingly argued by the appellant. Hence, arrows 30 and 31 shown in Figure 1 of D1 imply that a "session request" is received by hearing device 2 in accordance with feature (e), but D1 does not disclose which "processing unit" is actually responsible for receiving this request. It could be signal processing unit 14 or the "processor" running the software to embody operability control unit 3 as mentioned in the first sentence of paragraph [0136] of D1 or, further still, a processing unit of an external device (e.g. of remote control 19 shown in Figure 1 of D1 or even a processing unit of an unspecified device such as a smartphone).

3.1.3 Concerning **feature (j)**, the data exchange illustrated by arrow 30 shown in Figure 1 of D1 directly and unambiguously discloses that "session data" is received via the interface mentioned in point 3.1.1 above. Nonetheless, again, it is not disclosed *which* processing unit is indeed involved in this data exchange.

3.1.4 Relating to **features (f) to (i)**, the terms "secure connection" and "data encryption" mentioned in paragraph [0141] of D1 as well as the term "secure" used above arrow 30 referred to in point 3.1.3 above indicate that the data exchange depicted by that arrow 30 must concern either a symmetric or an asymmetric type of encryption. While the former type will normally imply the use of a single key, it is not necessarily the encryption type adopted in D1. Stated differently, D1 does not directly and unambiguously

disclose a "session key" in accordance with features (f) to (i).

3.1.5 In conclusion, the board considers features (e) and (j) not to be disclosed for the sole reason that there is no direct and unambiguous teaching in D1 that signal processing unit 14 *must* be involved in the data exchange illustrated by arrow 30 in Figure 1 of D1. In other words, regarding features (e) and (j), D1 does not disclose that (board's feature labelling)

(A) the receiving steps of features (e) and (j) are performed by the *same* processing unit that is also configured to compensate for a user's hearing loss according to feature (b).

In addition, features (f) to (i), in their entirety, are not directly and unambiguously disclosed in D1.

3.2 The respondent phrased the objective technical problem to be associated with **features (f) to (i)** and **feature (A)** as "to implement a secure communication between a hearing device for hearing loss compensation and another device" (emphasis as in the original).

However, feature (A) does not contribute to the solution of this technical problem. Moreover, features (f) to (i) do not necessarily lead to a "secure communication". These features only relate to obtaining and storing a "session key", encrypting that key based on another key that is stored in the hearing device and sending a session response. There is no mention of securing any "communication". In particular, the board acknowledges that the term "session" referred to in feature (j) implies that the "session" must be established *before* the receipt of the "session data" in

accordance with this feature takes place, but this session need not be encrypted or secure. The board also notes that claim 1 as granted does not specify any "other device" with which the claimed hearing device communicates, but agrees that such an "other device" can be deemed to be implicit from the term "session" mentioned in feature (j). In order to establish an objective technical problem, which is in fact derived from technical effects directly and causally related to the technical features of the claimed invention, the board deems it expedient to consider the technical effects of features (f) to (i) and of feature (A) separately:

3.2.1 Concerning **features (f) to (i)**, Reasons C1.2 of the appealed decision formulated the objective technical problem as how to "efficiently implement [a] secure communication between the hearing device and an external device". The appellant adopted the same objective technical problem.

The board does not find it credible that these features could *efficiently* implement a "secure communication". It is in particular not apparent which aspect of the secure communication should make the implementation more "efficient": this could relate, for instance, to power consumption, hardware requirements (hence costs) or time optimisation. Nonetheless, the board notes that both the appellant and the respondent (cf. point 3.2 above) use the expression "secure communication" in their formulation of the objective technical problem. Given this agreement between the parties on this aspect, the board will in the present case not question it, although, as set out in point 3.2 above, this is not necessarily mandated by claim 1 as granted. For the purpose of formulating a realistic objective technical

problem associated with features (f) to (i), the board emphasises that paragraph [0141] of D1 mentions a list of six alternatives to implement a "secure connection". The first one of these alternatives relates to the use of "data encryption". Given the limited number of alternatives, the board holds this to qualify as a direct and unambiguous teaching for the skilled reader that "data encryption" is used in the "secure connection" indicated with arrow 30 in Figure 1 of D1. Since claim 1 as granted does not use the term "secure" but, instead, employs the term "encrypt", the board finds it more appropriate to adopt the expression "encrypted communication" - instead of the expression "secure communication" as used by the parties - when formulating the objective technical problem (cf. point 3.4.1 below).

3.2.2 As regards **feature (A)**, Reasons C1.2 of the appealed decision does not mention an objective technical problem, for whatever reasons. The parties' submissions do not address an objective technical problem which takes into account this feature either. The board considers that feature (A) allows the total number of components in a hearing device to be reduced, given that it requires a single "processing unit" to perform several functionally independent tasks.

3.3 The board agrees with Reasons C1.2 of the appealed decision in so far as the group of features (f) to (i), on the one hand, and feature (A), on the other hand, are merely juxtaposed.

3.4 The respondent argued that Reasons C1.2 of the appealed decision represented an incorrect application of the "partial-problem approach".

The board does not agree. It acknowledges that the group of features (f) to (i) may allocate even more tasks to the same processing unit in this respect, but cannot see how this additional allocation would entail any synergistic technical effect. This is for the following reasons.

The respondent understood the distinguishing features to form a "true combination" due to the fact "that it is the same and single processing unit that compensates for hearing loss and performs the cryptographic operations of features (e)-(j)". It alleged that the interactions of the individual features resulted in a "synergistic effect". Nonetheless, the respondent did not provide an explanation of what this synergy actually entailed. In particular, for a synergy to be present, the functional interaction between the features must have a combined technical effect which is beyond the sum of the technical effects of the individual features. The respondent failed to identify such a combined technical effect. The "lightweight" solution suggested by the respondent in view of "one processor carrying out all of the steps" does not go beyond the sum of the individual contributions of each of the distinguishing features. In fact, the appellant convincingly pointed out in this regard that the "processing unit" according to granted claim 1 cannot, at the same time, compensate for a user's hearing loss in accordance with feature (b) and carry out the steps set out in features (e) to (g) and (i) to (j). This is because the latter steps are typically carried out when fitting the hearing device. Such fitting must however occur when the hearing device is in a "programming mode", which cannot co-exist with the hearing device's "normal operation mode". The respondent acknowledged this on page 7 of its written reply to the statement of

grounds of appeal, stating that a hearing aid's "programming mode" is normally initiated by "a press of a button on the hearing device" (cf. point 3.1.2 above). As argued by the appellant, the "processing unit" according to claim 1 as granted concerns only a multifunctional processor that runs different pieces of software at different times. Therefore, the board concurs that there is no synergy. Consequently, the problem-solution approach may indeed be carried out on the basis of several partial problems (PP).

3.4.1 Regarding **features (f) to (i)**, the board considers that the partial problem (**PP1**) to be associated with these features can be seen as "how to provide for a practical implementation of the encrypted communication between the hearing device and an external device in the system of D1".

The respondent argued that the board's objective technical problem included a pointer to the solution, in particular feature (g), because it contained the term "encrypted". By doing so, it however presented seemingly contradictory arguments when stating that the "data encryption" mentioned in paragraph [0141] of D1 merely implied that data was encrypted and decrypted, but not that a particular "session key" was encrypted as per feature (g) for future use in communicating session data. In any case, the board does not consider its objective technical problem to point to the solution of *encrypting the session key* with a hearing-device key as required in feature (g). An "encrypted communication" does not necessarily imply the use of an encrypted "session key". Such a key does not occur in asymmetric encryption schemes, for instance (cf. point 2.1 above). While the objective problem for use in the problem-solution approach must

be formulated such that it does not contain pointers to the solution, the board notes that this problem should not be formulated so generally as to circumvent indications in a prior-art document towards the claimed solution (**T 1019/99**, Reasons 3.3). In the case in hand, paragraph [0141] of D1 explicitly mentions the need for a "secure connection" when editing "operability data 5". It suggests "data encryption" and, more broadly, "other cryptographic methods for securing data connections" as possibilities for securing that connection. This points towards the use of encryption techniques to protect the communication between the hearing aid and the external device.

3.4.2 Concerning **feature (A)**, the underlying partial problem (**PP2**) can be framed as "how to reduce the total number of components needed for hearing device 2 of D1".

3.5 The board considers that the skilled person would have solved PP1 as well as PP2 in such a way that they would have arrived at the group of features (f) to (i) and at feature (A) without exercising any inventive step. The reasons for this are set out below.

3.5.1 Concerning problem **PP1**, the board agrees with the appellant that this problem is addressed to the person skilled in the field of "secure communications" instead of the one from the field of "hearing devices" as the respondent proposed. The appellant rightly observed that there are only two ways to encrypt a session, namely via public/private key pairs in *asymmetric* schemes or via *symmetric* key encryption. The appellant also correctly identified symmetric key encryption as the more suitable option for resource-constrained hearing devices compared to asymmetric schemes. This

aligns with the skilled person's common general knowledge in the field and the need for minimising computational overhead and battery consumption. The appellant further convincingly explained that securing a connection between two devices typically involves several steps:

- Initially, the devices must establish trust. This can be achieved by the hearing-device manufacturer embedding a "hearing device key" in accordance with feature (g) in the hearing device's memory, serving as a shared secret. During the fitting process, which is necessary to configure the hearing device to compensate for a user's hearing loss as per feature (b) and typically conducted by an acoustician using the hearing-device manufacturer's fitting software, the same "hearing device key" can be embedded in the software, enabling trust establishment with the external fitting device.

- Once trust is established, the "hearing device key" can be used to securely transmit a "session key" as mentioned in feature (i) to the external device.

- To generate this "session key", i.e. to "obtain" and "store" in accordance with feature (f), typically, a key-agreement protocol is used. For security and immediate availability, it is common practice to generate this key from data stored in the hearing device's permanent memory as per feature (h). The "hearing device key" then encrypts the "session key" as per feature (g) before it is transmitted to the external device as set out in feature (i).

The respondent argued that the appellant's line of argument as set out in point 3.5.1 above did not mandatorily lead to an *encryption key* being encrypted with *another key* as required by feature (g). Instead, it posited that, due to limited resources in a hearing device, the skilled person would have only envisaged encrypting the session each time with the same hardware key (i.e. the "hearing device key" as it is called in claim 1 as granted) and would have avoided encrypting a second key.

The board is not convinced by this, for several reasons:

First, the appellant correctly pointed out that the use of a second key, namely the "session key", is necessary to defend against well-known replay attacks. This aligns with the advantage pointed out in paragraph [0011] of the opposed patent itself. A "session key", used only for a particular session and discarded afterwards, is indeed standard practice for preventing such attacks. If only the "hardware key" is used for all encryption processes, its compromise would actually jeopardise the entire system's security. Using a "session key" that is changed for each session and encrypted with a separate key arguably minimises the impact of a compromised session key.

Moreover, as the appellant rightly emphasised, to minimise the possibility of the "session key" being compromised, it must be transmitted between the conversation partners in a secret way. The "session key" cannot be transmitted simply in plain text, otherwise eavesdroppers can readily obtain this key. The encryption of the "session key" by means of the hardware key however reflects standard practice to

ensure a safe transmission between those partners. In that regard, the board agrees with the respondent that encrypting a second key would be resource-intensive, but the appellant's approach addresses this by suggesting *symmetric* key encryption, which is normally less computationally burdensome and suitable for resource-constrained devices like hearing devices.

3.5.2 The respondent alleged that "D1 teaches away from the claimed solution by providing an*[sic]* non volatile memory NVM 4 having the operability data 5 with a different secure connection 30 than the connection 31 to the DSP 14 of Fig. 1".

The board considers the respondent's focus on NVM 4 and its secure connection in D1 to be misplaced here. It acknowledges that arrows 30 and 31 shown in Figure 1 of D1 relate, respectively, to the transmission of "operability data 5" (paragraph [0141] of D1) and of hearing-loss parameters or user preferences (paragraph [0140] of D1). Nonetheless, the need for a secure connection in the former transmission does not preclude the need for a secure connection in the latter transmission. The board notes in this context that hearing-loss parameters are often considered healthcare data and that their transmission is therefore normally subject to data-protection regulations. In any case, the board notes that the distinction between, on the one hand, "operability data 5" and, on the other hand, hearing-loss parameters (or user preferences) is not relevant for the construction of claim 1 as granted, given that the term "session data" in accordance with feature (j) does not allow to make that distinction.

3.5.3 Furthermore, the respondent highlighted the multitude of options for securing data connections as suggested

in paragraph [0141] of D1 and emphasised that each of these options encompasses myriads of practical implementation possibilities. It concluded that choosing between this vast number of options would be an "undue burden" for the skilled person, at least without granted claim 1 as a "roadmap".

However, this argument overlooks the key aspect that hearing device 2 shown in Figure 1 of D1 has already specific constraints and requirements, such as limited resources and the need for efficient and secure communications with an external device. As a result, the skilled person would have indeed focused on encryption schemes that are both efficient and widely recognised within the field. At the date of filing of the opposed patent, the Advanced Encryption Standard (AES), particularly AES-128, was arguably the most suitable candidate that met these criteria. While other options might technically exist, the skilled person would naturally have considered that standard to solve the objective problem posed.

3.5.4 The respondent further argued that claim 1 as granted did not use public-key encryption or AES but rather a "security architecture" or "protocol" that was defined by features (f), (g) and (i). This meant that any device that was not part of this "security architecture" or "protocol" could not communicate with the claimed "hearing device".

However, this argument must fail already for the reason that claim 1 as granted does not exclude the possibility of the hearing device communicating with other devices using different security protocols or mechanisms, like AES-128. It does not define a restrictive "security architecture" or "protocol" that

limits communication to only compatible devices.

3.5.5 In addition, the respondent argued that there were "many ways to get a particular key safely to a remote conversation partner" and specifically gave the examples of an "exchange of random numbers" and a "password exchange". In view of these alternatives, the respondent stated that the appellant's arguments regarding obviousness merely related to how the skilled person *could* but not to how they *would* have solved the underlying objective technical problem.

The respondent did not provide specific details on how these alternatives would work. This makes it difficult for the board to judge whether these alternatives are equally likely options to solve the objective technical problem as the symmetric encryption scheme suggested by the appellant. The board has nonetheless severe doubts that this would be so, because, to provide for some degree of secrecy, a random-number exchange must typically involve computationally intensive operations that actually might not be suitable for resource-constrained hearing devices. Moreover, password exchange, while simpler, is generally less secure than using a session key, as passwords can be intercepted or guessed. The skilled person would therefore not have considered the alternatives invoked by the respondent as being as technically viable as the symmetric encryption scheme. For this reason, the proposed solution would have been obvious to the skilled person at the relevant date. Even if the skilled person had considered the three alternatives to be equally viable, an inventive step could not be acknowledged. This is because the choice between these known alternative solutions would have been straightforward for the skilled person when trying to solve the above objective

problem.

3.5.6 As regards problem **PP2**, the skilled person would have immediately understood, based on their common general knowledge, that programming an already existing processing unit to perform *multiple* independent functionalities (instead of having dedicated processing units for at least some of those functionalities) represents one obvious way to solve the problem posed. Reasons C1.2 of the appealed decision correctly states that implementing hearing-device functions with a *single* processor constitutes a routine choice. In this situation, the skilled person would have selected the receiving steps underlying features (e) and (j) to be executed by the very same "processing unit" that already compensates for the hearing loss according to feature (b). The same applies to the steps according to features (g) to (i).

In this context, the appellant rightly referred to paragraph [0155] of D1. This paragraph states that the functional units described in the embodiments mentioned in D1 "may be realized in virtually any number of hardware and/or software components adapted to performing the specified functions". The respondent's argument that this paragraph taught away because it only concerned signal generating unit 6 and signal processor 14 and not, for instance, operability control unit 3 which "will disable or not disable hearing device 1 from functioning as a hearing device" (cf. paragraph [0136] of D1) could not convince, given that the particular configuration as considered by the respondent is a mere example. The appellant also correctly pointed at the expression "and so on" at the end of this paragraph to emphasise this even more.

3.6 In conclusion, the subject-matter of claim 1 of the main request does not involve an inventive step (Article 56 EPC).

4. *Auxiliary requests: claim 1 - inventive step*

4.1 Irrespective of any admittance considerations regarding the present auxiliary requests, the board considers that none of the amendments underlying **auxiliary requests 1 to 5** provides a remedy for the deficiency of the main request set out in point 3 above. The reasons for this are as follows.

4.1.1 Regarding **feature (k)**, the respondent acknowledged that this feature did not require to change the objective technical problem as set out for the main request. It further stated that encrypting some cryptographic key with a symmetric key was not disclosed in D1 and that paragraph [0141] of D1 mentioned several possibilities of implementing a secure connection, including "data encryption", "authentication schemes", "data packet identifiers" and "hashes". The respondent posited that it would not have been straightforward for the skilled person to choose a symmetric hardware key to provide for the secure connection in the system of D1 because they would have needed to choose between all those possibilities. In its view, there was no evidence proving that a *symmetric* encryption protocol would have been better for a hearing device. In particular, the respondent concluded that there is no reason why the skilled person would have adopted a symmetric implementation of the "hearing device key" according to feature (k).

Nonetheless, the respondent did not provide any alternative options apart from the "symmetric" or an

"asymmetric" schemes mentioned by the appellant, despite having been invited by the board to do so. The board shares the appellant's point of view that there are indeed only two general schemes for encryption at the disposal of the relevant skilled person, at least for encryption algorithms that involve an encryption key, like the "session key" used in the claimed hearing device. The skilled person, having been aware, based on their common general knowledge, of the fact that *symmetric* encryption schemes are typically faster than *asymmetric* ones, would certainly have preferred the former in the context of hearing devices. The appellant also convincingly pointed out that "authentication schemes" normally serve a different purpose than "data encryption", namely ensuring that a particular message was transmitted by the authentic sender instead of protecting against eavesdropping. The board therefore agrees with the appellant that it would have been straightforward for the skilled person, faced with the objective technical problem set out in point 3.4.1 above, to encrypt the session key in accordance with feature (g) based on a *symmetric* encryption scheme. This means that the "hearing device key" must be a symmetric one, as required by feature (k).

4.1.2 Concerning **feature (l)**, the respondent indicated that this feature did not require to change the objective technical problem either. It argued that the data communication such as the one between hearing device 1 and fitting apparatus 7 shown in Figure 1 of D1 did not necessitate that the hearing device includes its identifier. This was, in the respondent's view, because the communication partners could assume that they were always communicating with the same partner.

The board finds this argument to be entirely

speculative. It agrees instead with the appellant that any form of wireless communication between two devices over a telecommunication link will necessarily require a respective identifier for the devices (e.g. an IP address or a MAC address, for the latter see also paragraph [0045] of the opposed patent). Otherwise, a receiving device connected via a wireless link has no means for identifying the sender of a particular piece of information. This means that feature (l) is implied by the mere presence of "wireless" communications referred to in paragraph [0081] of D1.

4.1.3 As regards **feature (m)**, the respondent, referring to the well-known "mind willing to understand", emphasised that this feature focuses on decryption and that the board's objective technical problem needed to be changed to accommodate this. To do so, it was necessary to formulate the objective technical problem as "how to provide a secure connection to the hearing device [of D1]". To solve this reformulated objective technical problem, the skilled person would have, at best, taken *one* key in the external device and *one* (different) key in the hearing device, at least in the respondent's opinion.

Nevertheless, the appellant convincingly countered that an "encrypted communication" always implies a decryption step. This means that the board's objective technical problem as formulated in point 3.4.1 above does not need to be altered in view of feature (m). The board also considers that the allocation of two further tasks, namely the "decrypting" and "storing" steps in accordance with feature (m), to the *same* processing unit would have been a routine option for the skilled person, at least within the framework of a symmetric

encryption scheme.

4.1.4 In relation to **feature (n)**, the respondent stated that "fitting data" as mentioned in this feature differed from the "switching of a flag" as done in D1. It emphasised that, correspondingly, D1 differentiated between "operability data 5" and "hearing loss data". It considered that this feature achieved the technical effect of securely updating the hearing device.

The board understands the respondent's "switching of a flag" to refer to the selection of a value of either "0" or "1" for a specific bit, as set out in paragraph [0137] of D1. It agrees, however, with the appellant that claim 1 of auxiliary request 4 does not specify what happens with the "fitting data" and that the precise content of the "fitting data" in the context of feature (n) is not specified. The "operability data" causing the change of the value of that specific bit may indeed very well be considered, as set out by the appellant, to be "fitting data" as per feature (n), the more so since that specific bit defines whether or not the hearing device is "functionable" (cf. paragraph [0137] of D1). The board therefore considers feature (n) to be already disclosed in D1 (see also paragraph [0141]: "fitting software 9" and "operability data 5").

4.1.5 Concerning **feature (o)**, the respondent alleged that this feature formed a "true combination" that went beyond the disclosure of D1. It submitted in this respect that the "switching of a flag" in this document determined whether the hearing device used in the system of D1 had a beamforming functionality.

The board acknowledges that paragraph [0145] of D1, to

which also the appellant referred, may be understood such that the use of an advanced beamforming algorithm is allowed or disabled depending on "operability data". However, this paragraph further specifies that "other functionalities" can be allowed or disabled as well. This means in turn that the "operability data" is not necessarily restricted to turning on the beamforming functionality in the system of D1. Moreover, for the reasons mentioned in point 3.5.2 above, the need for a secure connection in transmission 30 shown in Figure 1 of D1 does not preclude the need for a secure connection in the transmission 31 shown in that Figure. The board can recognise no "synergy" induced by feature (o), the more so since the respondent did not refer to any specific synergistic effect in this context. As set out in paragraph [0140] of D1, transmission 31 concerns the hearing device's adjustment to the "hearing needs and preferences of the hearing device user". To reduce data overhead, it would thus have been straightforward for the skilled person to secure transmissions 30 and 31 in the same way. By doing so, they would have inevitably arrived at feature (o).

4.2 Therefore, none of the five auxiliary requests is allowable under Article 56 EPC either.

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