Internal distribution code:

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

Datasheet for the decision of 11 February 2025

Case Number: T 0454/23 - 3.5.05

Application Number: 19153306.6

Publication Number: 3493464

IPC: H04L9/32, H04R25/00, H04L9/08

Language of the proceedings: EN

Title of invention:
Client device with certificate and related method

Patent Proprietor:
GN Hearing A/S

Opponent:
Oticon A/S

Headword:
Authentication messages for hearing devices/GN HEARING

Relevant legal provisions:
EPC Art. 56

Keyword:
Inventive step - (no): determination of the objective technical problem under the established problem-solution approach - conclusions of T 495/91 not followed

Decisions cited:
G 0001/19, R 0009/14, T 0001/80, T 0495/91, T 1861/17, T 1830/22

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 0454/23 - 3.5.05

D E C I S I O N
of Technical Board of Appeal 3.5.05
of 11 February 2025

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:	GN Store Nord A/S Lautrupbjerg 7 2750 Ballerup (DK)
Decision under appeal:	**Interlocutory decision of the Opposition Division of the European Patent Office posted on 23 December 2022 concerning maintenance of the European Patent No. 3493464 in amended form.**

Composition of the Board:

Chair	K. Bengi-Akyürek
Members:	P. Tabery
	F. Blumer

Summary of Facts and Submissions

I. The appeal lies from the decision of the opposition division to maintain the opposed patent in amended form according to an "auxiliary request 1".

The opposition division found that the subject-matter of claim 1 as granted did not involve an inventive step (Articles 100(a) and 56 EPC) over document D1 in combination with the skilled person's common general knowledge evidenced by document D12.

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

D1: EP 2 760 225 A1

D12: S. Vaudenay: "A Classical Introduction to Cryptography: Applications for Communications Security", Springer, 2006, pp. 150 to 153.

III. Oral proceedings before the board were held on 11 February 2025. The final requests of the parties were as follows:

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

- The respondent-proprietor (henceforth "the proprietor") requested that the appeal be dismissed, i.e. that the patent be maintained as found allowable by the opposition division.

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

IV. Claim 1 of the **patent as maintained** by the opposition division reads as follows (board's labelling):

(a) "A client device (10) for hearing device communication, the client device (10) comprising
(b) a processing unit;
(c) a memory unit; and
(d) an interface,
(e) the memory unit having a client device key (182) and a client device certificate (106, 107) stored thereon,
characterized in that
(f) the processing unit is configured to
- receive a connection response (412) comprising a hearing device identifier (112) via the interface;
(g) - generate one or more keys including a certificate key based on the hearing device identifier (112) and the client device key (182);
(h) - obtain an authentication message (424) based on the certificate key and the client device certificate (106, 107), and
(i) - transmit the authentication message (424) via the interface,
(j) wherein the processing unit is configured to obtain a session identifier (180), and
(k) wherein to generate one or more keys comprises to generate a hearing device key based on the hearing device identifier (112) and the client device key (182), and
(l) to generate a common secret based on the hearing device key and the session identifier (180),
(m) wherein the certificate key is based on the common secret and a certificate value."

Reasons for the Decision

1. The present patent concerns some sort of authentication for the communication between a "client device" (e.g. fitting device) and a "hearing-aid device". The authentication is performed using certificates.

2. Inventive step (Article 56 EPC)

2.1 It is common ground that document **D1** does not explicitly disclose **features (g) to (m)**, denoted F1.6, F1.7, F1.8, F2.1, F2.2, F2.3 and F3 in the decision under appeal. As to **features (h) and (i)**, denoted F1.7 and F1.8, the board holds that the actual difference vis-à-vis document D1 resides in the generation of the "certificate key" in accordance with feature (g) which is then used in the subsequent steps.

2.2 The board concurs with the opponent that claim 1 fails to specify the concrete way of calculating the certificate key (C_KEY), the session identifier (S_ID), the hearing-device key (HD_KEY) and the common secret (CS). Thus, claim 1 indeed lacks elements which are indispensable for deriving the alleged technical effect. Instead of specifying the actual cryptographic operations performed, the respective features of claim 1 merely define that the resulting element is generated "based on" the initial elements. Thus, claim 1 encompasses technically sensible scenarios where the "based on" relationship is implemented by merely concatenating the respective keys, i.e. "gluing" them together. Consequently, the subject-matter of claim 1 comprises embodiments where the respective elements are generated in ways which are entirely unsuitable to enhance the security of the underlying hearing-aid system. Therefore, the features of claim 1

which are not disclosed in document D1 do not cause a technical effect which is credibly achieved over the entire breadth claimed (see e.g. **G 1/19**, cited by the proprietor, Reasons 49, 82 and 124). The board understands that established authentication procedures and the respective messages involved, as such, were commonly known to the skilled person in the field of data communications at the relevant date.

2.3 As to the objective technical problem solved by present claim 1, the proprietor contended that the combination of features (g) to (m) provided "a robust mechanism for improve*[sic]* security of an authentication message by a client device" and referred essentially to the conclusions drawn in **T 495/91**, Reasons 4.2, according to which an objective definition of the problem to be solved by the invention should normally start from the problem described in the application (original text: "*[...] ist dabei regelmäßig von der im Streitpatent formulierten Aufgabe auszugehen.*").

However, according to the problem-solution approach as defined in **T 1/80** (cf. headnote I) (see e.g. also **G 1/19**, Reasons 26; **R 9/14**, Reasons 2.1.1) and in the Guidelines for Examination in the EPO (see part G, chapter VII, section 5, items (i) and (ii)), the formulation of the "objective technical problem" should always be done *after* having identified the closest prior art (i.e. the suitable starting point) for the assessment of inventive step (see e.g. **T 1861/17**, Reasons 3.4). As a consequence, the conclusions of **T 495/91** do not appear to be reconcilable with the well-established problem-solution approach. To avoid any misunderstandings: of course, by coincidence, the problem described in the application itself, i.e. also called the "subjective problem", may well correspond to

the objective problem formulated later on the basis of the selected closest prior art; for example, if the suitable starting point is already cited in the application itself. But, the established problem-solution approach does not imply that, for the purposes of determining the objective technical problem, one should "normally start from the problem described in the application".

2.4 With respect to the proprietor's argument that the necessary cryptographic operations were already mentioned in the present description, the board recalls that the description cannot be used to read unclaimed features into the claim. Also, the argument that the "patent is its own dictionary" invoked by the proprietor during the oral proceedings before the board cannot succeed, since neither the wording of Article 69(1) EPC ("*the description and drawings shall be used to interpret the claims*") nor the established jurisprudence of the Boards of Appeal can provide a basis for such a strict application of the alleged concept of the "patent as its own dictionary" (see e.g. **T 1830/22**, Reasons 1.4).

2.5 Moreover, the proprietor argued that the claimed features related to an enhancement of an aspect within a larger system and thus had to be understood in its context. This also fails to convince the board, since it is established case law that the technical effect needs to be derived by the skilled person on the basis of the claimed invention.

2.6 Furthermore, the board is also not persuaded by the proprietor's argument that the cryptographic nature and the functioning of the claimed cryptographic steps was defined by the "cryptographic keys" mentioned therein.

These had to be understood in the light of the present description (referring to paragraph [0014] of the opposed patent) as being generated by cryptographic algorithms.

The board disagrees. As also noted by the opponent, the mere names given to the respective cryptographic keys are insufficient for defining their *actual* use. In addition, the cited passage of paragraph [0014] in fact discloses that "a cryptographic key [...] determines a functional output of a cryptographic algorithm" and thus refers only to the *intended* use of the underlying cryptographic keys.

2.7 Lastly, the proprietor submitted that the use of the multiple cryptographic steps defined in claim 1 made it harder to attack the underlying "authentication procedure".

Also this argument fails to sway the board. Claim 1 does by no means specify an "authentication procedure". It, at best, refers to obtaining and transmitting an "authentication message" by the claimed "client device" without even indicating to which unit this message is actually sent and how an alleged authentication process is subsequently performed. Therefore, only based on pure speculation, the skilled reader could derive which impact the claimed features might have on an undefined "authentication procedure". In other words, the wording of claim 1 constitutes a mere compilation of several unspecified calculations of some unspecified security keys without even indicating for which purpose (e.g. confidentiality, message authentication, data integrity, etc.) those keys (such as the claimed "common secret" or "certificate key") are finally used in the underlying communication system.

2.8 Consequently, the subject-matter of claim 1 does not involve an inventive step in view of document D1 and the skilled person's common general knowledge.

3. In view of the above, the patent as maintained by the opposition division is not allowable under Article 56 EPC.

4. Since there are no further claim requests on file, the opposed patent has to be revoked.

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