Internal distribution code:

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

Datasheet for the decision of 7 July 2025

Case Number: T 0521/23 - 3.5.05

Application Number: 16798132.3

Publication Number: 3542554

IPC: H04R25/00

Language of the proceedings: EN

Title of invention:
Method of controlling access to hearing instrument services

Patent Proprietor:
Sonova AG

Opponent:
Oticon A/S

Headword:
Access-control method for a hearing instrument/SONOVA

Relevant legal provisions:
EPC Art. 56, 100(a)
RPBA 2020 Art. 12(4)

Keyword:
Inventive step - main request, auxiliary requests 1 to 4 (no): obvious implementation of an administrative policy
Admittance of claim request filed on appeal - auxiliary request 5 (no): no reasons provided for late filing

Decisions cited:
T 0939/92, T 0641/00

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 0521/23 - 3.5.05

D E C I S I O N
of Technical Board of Appeal 3.5.05
of 7 July 2025

Appellant: (Opponent)	Oticon A/S Kongebakken 9 2765 Smoerum (DK)
Representative:	Cohausz & Florack Patent- & Rechtsanwälte Partnerschaftsgesellschaft mbB Bleichstraße 14 40211 Düsseldorf (DE)
Respondent: (Patent Proprietor)	Sonova AG Laubisrütistrasse 28 8712 Stäfa (CH)
Representative:	Schwan Schorer & Partner mbB Patentanwälte Bauerstraße 22 80796 München (DE)
Decision under appeal:	**Decision of the Opposition Division of the European Patent Office posted on 3 January 2023 rejecting the opposition filed against European patent No. 3542554 pursuant to Article 101(2) EPC.**

Composition of the Board:

Chair	K. Bengi-Akyürek
Members:	K. Peirs
	C. Heath

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 documents:

D2: US 2016/0173278 A1

D6: *Computer access control*, Wikipedia online encyclopaedia, revision of 30 October 2016 Retrieved on 14 September 2022

D7: *Principle of least privilege*, Wikipedia online encyclopaedia, revision of 17 March 2016. Retrieved on 14 September 2022

D8: *Access control matrix*, Wikipedia online encyclopaedia, revision of 14 October 2016. Retrieved on 14 September 2022

II. Oral proceedings before the board were held on 7 July 2025. The parties' final requests were as follows:

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

- The respondent (proprietor) 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 (i.e. **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 method of controlling access of a client (42) to a service of a hearing instrument (10), the method comprising the steps of:
(b) requesting access of the client (42) to the service of the hearing instrument (10) by providing a client authenticator to the hearing instrument (10);
(c) authenticating the client (42) based on a validation of the provided client authenticator by the hearing instrument (10);
characterized in that
(d) upon successful authentication, comparing a security level associated with the service requested by the client (42) with a highest security level assigned to the client (42) by the hearing instrument (10),
(e) wherein the security level is selected from a plurality of hierarchically structured security levels, and
(f) granting access of the client (42) to the service of the hearing instrument (10), if the requested security level is below or equal to the highest

security level assigned to the client (42)."

IV. Claim 1 of **auxiliary request 1** differs from claim 1 of the main request in that features (d) and (f) are replaced, respectively, by the following features (board's feature labelling and highlighting, the latter reflecting amendments vis-à-vis, respectively, features (d) and (f)):

(g) "upon successful authentication, comparing, by the hearing instrument (10), a security level associated with the service requested by the client (42) with a highest security level assigned to the client (42) ~~by the hearing instrument (10)~~,"

(h) "granting, by the hearing instrument (10), access of the client (42) to the service of the hearing instrument (10), if the requested security level is below or equal to the highest security level assigned to the client (42)."

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

(i) "wherein providing a client authenticator comprises granting a authorization to each client (42) and storing hearing instrument (10) service authorizations granted to clients (42) on the hearing instrument (10); wherein the hearing instrument rejects the access to the requested hearing instrument service, if the security level assigned to the client (42) is not at least as high as the security level associated with the service request, wherein an authorization comprises at least the client authenticator and the highest security level assigned to the client, and wherein

a client (42) privileged by an authorization to access a certain security level is also privileged to access all security levels below it".

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):

(j) ", and wherein the method further comprises: defining a plurality of authorization methods and assigning to each of the security levels at least one of the authorization methods in such a manner that each authorization method assigned to a certain security level is different to the authorization methods assigned to the other security levels, wherein each authorization method is for granting an authorization to a client to access hearing instrument service(s) assigned with at the respective security level".

VII. Claim 1 of **auxiliary request 4** differs from claim 1 of auxiliary request 3 in that it comprises, at the end, the following feature (board's feature labelling):

(k) ", wherein the authorization methods include at least one of: authorization by a specific user gesture, authorization by predefined shared secrets, authorization via a third entity trusted by the hearing instrument, and authorization by default".

VIII. Claim 1 of **auxiliary request 5** differs from claim 1 of auxiliary request 3 in that it comprises, at the end, the following feature (board's feature labelling):

(l) ", and wherein a first security level, corresponding to a firmware update, is assigned with a first authorization method, a second security level, corresponding to a fitting process, is assigned with a second authorization method, and a third security level, corresponding to a remote control access, is assigned with a third authorization method".

Reasons for the Decision

1. *Technical background*

1.1 The opposed patent concerns a method of controlling access to services provided by a hearing instrument, such as volume control or allowing fitting parameters to be read from and written to the hearing instrument.

1.2 According to the patent, modern hearing instruments can connect to various external client devices, such as smartphones or fitting stations. As set out in paragraph [0003] of the patent specification, a problem with prior-art systems is said to be that, once connected, a client's applications may have full access to the hearing instrument. This is described as posing a safety risk, as it grants even non-trusted applications the ability to modify safety-critical hearing-instrument configurations.

1.3 To address this, the opposed patent proposes an access-control method that is enforced on the hearing instrument itself:

1.3.1 As illustrated conceptually in Figure 2 of the patent (reproduced below), this method introduces an "Access

Control" layer between a client's application and the various services of the hearing instrument. The method defines a plurality of services (e.g. service 1, service 2, service 3), each assigned a security level from a set of hierarchically structured security levels based on its criticality.

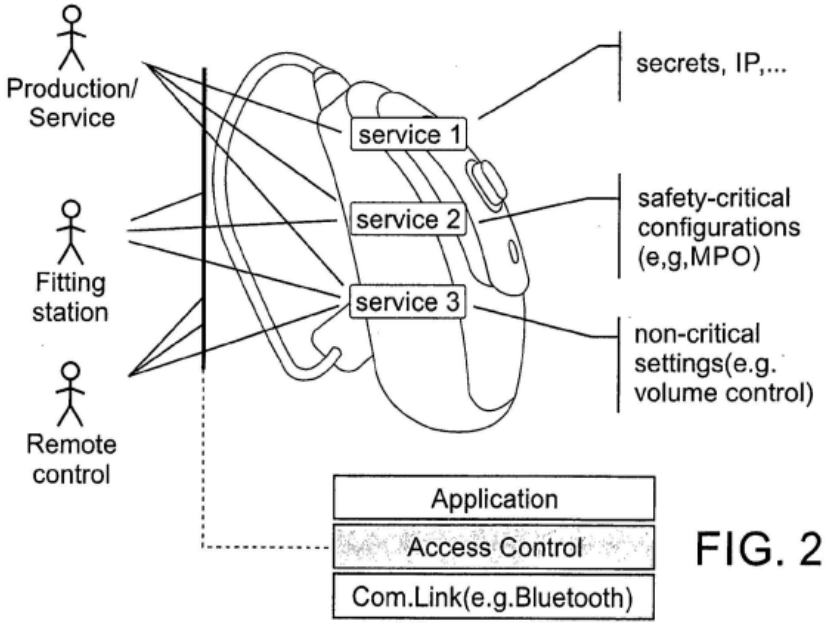

FIG. 2

1.3.2 In a typical use scenario, a client, such as a fitting station or a remote-control application, requests a service from the hearing instrument (10). Upon such a request, the hearing instrument (10) authenticates the client and compares the security level of the *requested* service with a "highest security level" that has been *assigned* to that specific client. The opposed patent provides examples of such services, including *non-critical* services like remote control or volume control, *moderately critical* services like adjusting fitting parameters and *highly critical* services such as performing a firmware update. As shown in the scheme of Figure 13 of the opposed patent (also reproduced below), access is granted only if the security level assigned to the client is at least as high as the

security level required for the service.

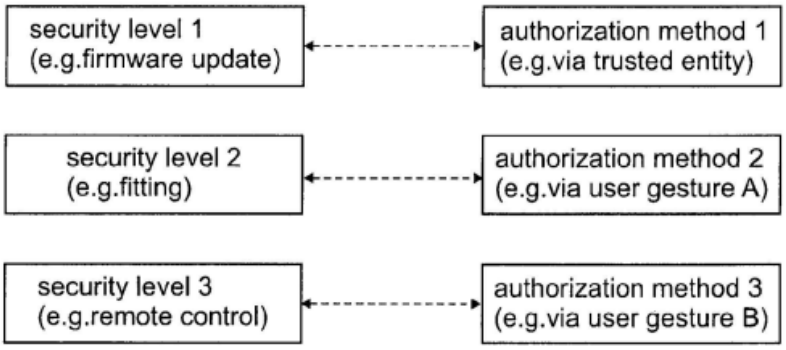

FIG. 13

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

2.1 Reasons 4.1 of the appealed decision considers document **D2** to be a suitable starting point for assessing inventive step in relation to claim 1 of the main request. The opposition division found this document to disclose **features (a) to (c)**. The parties did not contest this and neither does the board. As a result, **features (d) to (f)** are acknowledged as distinguishing features over D2.

2.2 In relation to the technical effect to be associated with features (d) to (f), the board makes the following observations:

2.2.1 The respondent submitted that the technical effect to be attributed to the distinguishing features was a "simplification" of the access-control scheme, leading to "low resource requirements". In support of this, it argued that the skilled reader would always understand the invention in the context of a "hearing instrument", which was, in the respondent's opinion, an inherently

resource-constrained device, a fact that it considered to be confirmed by document D2 itself (see D2, paragraph [0004]). This echoes Reasons 4.2 of the appealed decision, in which the opposition division, referring to paragraph [0015] of the opposed patent, found the technical effect of the distinguishing features to be "client specific service access requiring low resources". In that regard, the respondent argued that the claimed method, which relied on a single comparison against a client's "highest security level" as per feature (d), was inherently simpler than checking a detailed list or matrix of rights for *each* client, the latter being a method it considered to be representative of the skilled person's common general knowledge as exemplified in document **D8**. During the oral proceedings before the board, the respondent attempted to concretise this by giving an example of managing several thousands of hearing-care professionals (HCPs) via a simple classification scheme where all HCPs share the same security level.

2.2.2 The board finds these arguments generally unconvincing. These arguments rely on reading limitations into a claim which are not supported by its wording. They require the skilled reader of present claim 1 to understand the claim in the specific context of a *resource-limited* device and to assume that the claimed architecture is necessarily implemented in its *simplest* form. In view of the wording of feature (b), the skilled reader of claim 1 could only speculate as to whether the actual "service" requested by the "client" (being relevant to the performance of method step (d)) is notified by the "client authenticator", as advocated by the respondent, or by another, yet undefined, data message. In addition, it is not derivable from claim 1 whether, in feature (e), the

"security level" to be selected (arguably by an administrator according to the respondent) from many security levels is supposed to refer to the "security level associated with the *service request*" or to a "security level assigned to the *client*", so that the skilled reader cannot even establish whether the "client" is necessarily associated with more than one security level (i.e. "highest security level").

However, the assessment of inventive step must be based on the whole scope claimed, not on a preferred or commercially advantageous embodiment. The board notes the respondent's reference to the "business success of respective products" but considers this to be irrelevant to the assessment of inventive step, particularly where a credible technical effect is not established. The respondent's further example of simplifying the management of several thousands of HCPs by assigning them all to a *single* security level is equally unpersuasive. As the appellant correctly observed, claim 1 as granted does not relate to such a grouping or classification of clients: this is merely another example of an argument based on a specific, undisclosed implementation rather than on the technical features of the claim itself.

2.2.3 More specifically, the board cannot acknowledge the alleged technical effects of "simplification" or "low resource requirements" as being credibly achieved over the entire scope of claim 1. This is because claim 1 is silent about the resource requirements of the claimed method. It limits neither the number of security levels in the "plurality", nor the frequency with which the comparison steps are actually conducted. Hence, an implementation with, for example, a complex hierarchy or involving frequent access requests could in fact be

resource-intensive. Furthermore, claim 1 as granted does not preclude the possibility of "offloading" computationally intensive tasks to a more powerful peripheral device, such as a smartphone. For this reason, the respondent's argument that "the skilled reader would not consider complex algorithms when dealing with a hearing instrument" must be discarded.

Similarly, as regards the technical effect considered by the opposition's division in Reasons 4.2 of the appealed decision (cf. point 2.2.1 above), claim 1 as granted does not require that access be "client specific" in any technically meaningful way, as this would be achieved even if all clients were assigned the same security level (cf. the last sentence of point 2.2.1 above).

2.2.4 In view of the above, the board cannot derive any credible technical effect of "simplification" or "reduced resource usage" from the distinguishing features (d) to (f). At most, the effect of these features can be seen as the definition of a particular access-control policy (see also the description as filed, e.g. page 5, line 20 to page 6, line 8). This policy dictates that access is granted if a "requested security level" is below or equal to the "highest security level assigned to the client". The board concurs with the appellant's argument, advanced during the oral proceedings before the board, that such a policy is primarily administrative in nature and that its advantages, if any, consequently lie on the *administrative* rather than the *technical* side.

2.2.5 Based on the effect identified in point 2.2.4 above and the well-established COMVIK approach (cf. **T 641/00**, headnote II), the objective technical problem consists

therefore, at most, in the technical implementation of this specific, non-technical security policy on the hearing instrument disclosed in document D2.

2.3 The board holds that the skilled person would have arrived at the solution defined by the distinguishing features in an obvious manner:

2.3.1 Schemes that implement access control using a hierarchy of different permission levels are a fundamental part of the skilled person's common general knowledge in the field of computer science. Such schemes are analogous to common digital-rights-management systems or tiered access models, such as those for airline lounges or different health-insurance plans. The respondent's procedural challenge during the oral proceedings before the board, citing **T 939/92** (Reasons 2.3) and arguing that common general knowledge must be proven if contested, is not persuasive. The board is entitled to consider such fundamental technical principles to be part of the skilled person's common general knowledge. In any event, the appellant did provide documentary evidence of this common general knowledge in the form of **D6** and **D7**. This common general knowledge is broad and encompasses a spectrum of implementation models. That spectrum in turn includes highly granular models aimed at fulfilling the "Principle of Least Privilege" as described in **D7**, which grant subjects only the minimum permissions necessary. It also includes simpler, more coarse-grained hierarchical structures. The respondent's argument that the claimed method is distinguished from the "Principle of Least Privilege" because it provides coarse-grained access is noted. However, this argument does not distinguish the claimed invention from the skilled person's common general knowledge as a whole. It merely serves to situate the

claimed method within the known spectrum of possible access control implementations, at the simpler, more coarse-grained end of that spectrum.

2.3.2 The board therefore considers that the skilled person, starting from D2 and seeking to implement the security policy defined in the objective technical problem (see point 2.2.5 above), would have been motivated to use a *hierarchical* model. The respondent's argument that the common general knowledge pointed only towards a complex matrix is unconvincing given the ubiquity of hierarchical access-control models. The board further concurs with the appellant that document D2 itself, in paragraph [0038], hints at a multi-level security architecture by disclosing a basic connection authenticated by a pre-established link (such as Bluetooth® pairing) on top of which a further service is authenticated by a digital signature. The respondent's counter-argument that this merely discloses two sequential authentication steps and not a hierarchy is not accepted. These are two distinct methods for accessing services, implying, typically, different levels of trust and security.

2.3.3 The respondent's main defence, namely that the skilled person would have been deterred from applying a concept from the field of computer science due to the resource constraints of a hearing instrument, may have convinced the opposition division (cf. Reasons 4.2 of the appealed decision, last sentence) but in the board's view is without merit. As established in point 2.2.3 above, the claimed method could involve "outsourcing" in the sense that it is at least partially "offloaded" to a more powerful peripheral device: it is not required to be executed *solely* on a hearing instrument. Even if it were, the board considers that the skilled

person would have employed obvious strategies to mitigate resource limitations, such as optimising the security features to minimise their resource footprint or tailoring these features to the specific needs of the hearing device and its user.

The respondent argued that "outsourcing" tasks to a connected device would have led the skilled person away from the claimed invention. This, however, was a mere allegation for which no substantive reasoning was provided. Moreover, the argument misconstrues the board's reasoning: the board did not suggest "outsourcing" as a step towards the claimed invention, but rather as an obvious alternative strategy available to the skilled person at the relevant date for mitigating resource constraints. The existence of such an obvious alternative undermines the respondent's argument that their specific on-device solution required an inventive step. The respondent's own argument that only the most critical steps (e.g. those underlying features (d) and (f)) must be carried out on the hearing instrument itself implicitly acknowledges that other steps can be externalised, further supporting the board's view.

2.3.4 The board therefore holds that the solution defined by features (d) to (f) would have been an obvious course of action for the skilled person based on the disclosure of document D2 in combination with their common general knowledge.

2.4 Hence, the subject-matter of claim 1 of the main request does not involve an inventive step (Article 56 EPC). The ground for opposition under Article 100(a) in conjunction with Article 56 EPC therefore prejudices

the maintenance of the patent as granted.

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

3.1 Concerning **auxiliary request 1**, the board notes that **features (g) and (h)**, in essence, specify that the "comparing" and "granting" steps in accordance with features (d) and (f) of claim 1 of the main request are performed "by the hearing instrument". The respondent indicated that this claim request was filed as a mere "clarification". The board notes however that its reasoning for the main request provided in point 2.3 above has already taken into account this "clarification". It emphasises that the specification "by the hearing instrument" in features (g) and (h) does not exclude the "outsourcing" possibility mentioned in point 2.3.3 above, given that this specification does not require the respective steps to be executed *solely* by the hearing instrument.

3.2 In relation to **auxiliary request 2**, the parties mainly focused on the "storing" part of **feature (i)**, i.e. the phrase "storing hearing instrument (10) service authorizations granted to clients (42) on the hearing instrument (10)".

3.2.1 During the oral proceedings before the board, the respondent submitted that this feature provided the technical benefit of simplifying access for recurring requests from the same client. It argued for a "two-round" scenario where, after a first successful authorisation, subsequent access requests would be faster as the "hearing instrument" mentioned in claim 1 of auxiliary request 2 could use the stored authorisation, thus avoiding a new, full authorisation

procedure.

3.2.2 The board is not convinced by this argument. First, as the appellant rightly pointed out, claim 1 of auxiliary request 2 does not necessarily define a multi-session process for a "returning" client. The benefit alleged by the respondent is therefore based on a scenario that is not mandatorily reflected in the claim, making the effect speculative. Secondly, the argument relies on the term "storing", implying a certain level of persistence. However, as the board finds, "storing" could be satisfied by a transient storage in volatile memory (RAM), which could subsequently be erased moments later. In such an embodiment, which is covered by claim 1, no benefit for subsequent access requests would be achieved. The effect is therefore not credible over the whole scope claimed. Thirdly, the appellant correctly observed that this type of behaviour, i.e. storing keys to simplify reconnection, constitutes standard practice in wireless-system protocols like Bluetooth®, which is explicitly mentioned as a possible communication method in paragraph [0052] of D2. The alleged effect is therefore already achieved by the normal implementation of the prior-art schemes.

3.3 In relation to **auxiliary request 3** and **feature (j)** defining a plurality of authorisation methods that are assigned to different security levels, the board observes the following:

3.3.1 The respondent argued that this feature made the claimed method "more efficient" and "secure" by allowing the authorisation method in accordance with feature (j) to be adapted to a certain security level. During the oral proceedings before the board, it submitted that this feature explained how the "highest

security level" was attributed to a client, suggesting a trade-off between the client's "trust level" and the complexity of the algorithm underlying the associated authorisation method.

3.3.2 This argument is not persuasive. Adding a plurality of authorisation methods does not inherently lead to a simpler, more efficient or less resource-intensive system. It could, on the contrary, even increase processing complexity, namely where different authorisation methods are used for different levels of security. Regardless of the fact that the alleged effects are not credibly achieved, the board considers that the matching of a stronger authorisation method to a more critical operation to represent a standard, obvious design choice for any skilled person implementing a security system.

3.4 Concerning **auxiliary request 4** and **feature (k)**, listing examples of the authorisation methods mentioned in feature (j), including "authorisation by default", the board makes the following observations:

3.4.1 The respondent's allegation of a "synergy" between the authorisation-method examples mentioned in feature (k) and the "plurality of hierarchically structured security levels" in accordance with feature (e) is unsubstantiated. The board finds these two features to constitute a mere juxtaposition of well-known implementation measures.

3.4.2 Moreover, as the appellant rightly argued, feature (k) cannot contribute to an inventive step, for the following reasons.

The inclusion of the example "authorisation by default"

in feature (k) implies, according to paragraph [0051] of the opposed patent, that in fact *any* client could be granted a minimum level of access unconditionally, which however contradicts the goal of a secure, tiered system and appears to defeat the very purpose of the invention as set out in point 1.2 above. Moreover, the appellant correctly argued that document D2 already discloses the use of different security methods for different services: a first method for the Bluetooth® connection and a second, potentially more secure method (i.e. based on a digital signature) for a subsequent service request. The concept of using different methods is therefore already known from the prior art.

3.5 In consequence, auxiliary requests 1 to 4 are not allowable under Article 56 EPC, either.

4. *Auxiliary request 5: admittance*

4.1 In relation to **auxiliary request 5**, the board observes that this request was filed for the first time with the respondent's written reply to the statement of grounds of appeal. As such, it constitutes an "amendment" within the meaning of Article 12(4), first sentence, RPBA.

4.2 The board exercised its discretion not to admit auxiliary request 5 into the proceedings for the reasons set out below.

4.2.1 The primary reason for this decision is that the respondent failed to provide any justification for the late filing of this claim request. Under Article 12(4), third sentence, RPBA, reasons must be provided for submitting the amendment only at the stage of appeal proceedings. Despite being explicitly invited to do so,

the respondent provided no arguments in favour of admittance. In particular, it provided no reasons why this request was not submitted earlier, for instance during the opposition proceedings.

4.2.2 The board notes that the appellant objected to the admittance of this claim request on the grounds that it was filed too late, was not convergent with auxiliary request 4 and was based on passages from the description rather than the claims as granted. While the board sees some merit in these objections, its decision in this regard is primarily based on the respondent's aforementioned failure to provide some justification for the late filing.

4.2.3 Furthermore, the board has doubts as regards the *prima facie* allowability of auxiliary request 5 under Article 56 EPC: the proprietor did not indicate any technical effect which the amendment underlying claim 1 of auxiliary request 5 would credibly achieve and the board cannot immediately see such an effect either.

4.3 Hence, the board decided not to admit auxiliary request 5 into the appeal proceedings (Article 12(4), second 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