BESCHWERDEKAMMERN DES EUROPÄISCHEN PATENTAMTS | **BOARDS OF APPEAL OF THE EUROPEAN PATENT OFFICE** | **CHAMBRES DE RECOURS DE L'OFFICE EUROPÉEN DES BREVETS**

Internal distribution code:

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

Datasheet for the decision of 10 February 2026

Case Number:	T 0151/24 - 3.5.05
Application Number:	16202920.1
Publication Number:	3334190
IPC:	H04R25/00
Language of the proceedings:	EN

Title of invention:
Hearing devices, user accessory devices and method for updating a hearing device configuration

Patent Proprietor:
GN Hearing A/S

Opponent:
Oticon A/S

Headword:
Isolated islands of cryptography II/GN HEARING

Relevant legal provisions:
EPC Art. 100(a), 111(1), 56
RPBA 2020 Art. 11

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

Keywords:
Inventive step - main request and 1st to 4th auxiliary requests (no): equally likely alternatives
Remittal to the opposition division (no): no "special reasons"

Decisions cited:
G 0001/24, T 1924/20, T 1465/23, T 2027/23

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 0151/24 - 3.5.05

DECISION
of Technical Board of Appeal 3.5.05
of 10 February 2026

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)	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 30 November 2023 rejecting the opposition filed against European patent No. 3334190 pursuant to Article 101(2) EPC.**

Composition of the Board:

Chair	K. Bengi-Akyürek
Members:	K. Peirs
	R. Romandini

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 deemed that neither the ground for opposition under Article 100(a) EPC in conjunction with Articles 54 and 56 EPC nor the one under Article 100(b) EPC prejudiced the maintenance of the opposed patent as granted.

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

D1: US 2012/0140962 Al;
D3: "Public key certificate", Wikipedia, The Free Encyclopedia, revision of 28 November 2016.

II. Oral proceedings before the board were held on 10 February 2026.

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

The respondent (patent proprietor) requested that

- as a **main request**, the appeal be dismissed;
- as an auxiliary measure, the patent is maintained in amended form according to one of the **auxiliary requests** labelled as **A1 to A4**;

and that

- the case be remitted to the opposition division in the event that the main request is found not to meet the requirements of the EPC.

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, performed at a hearing device (8), for updating a hearing device configuration at the hearing device (8) of a hearing system (1),
(b) the hearing system (1) comprising the hearing device (8),
(c) a fitting device (2) configured to be controlled by a dispenser, and
(d) a server device (4),
characterized in that the method comprises:
(e) - receiving (S101) a configuration package (402) and a configuration authentication package (502),
(f) the configuration authentication package (502) comprising a dispenser certificate (506) and authentication data;
(g) - determining (S102) if an update criterion is fulfilled,
(h) wherein the update criterion is based on verifying the dispenser certificate comprised in the configuration authentication package (502),
(i) wherein verifying (S102a) the dispenser certificate (506) comprises:
- decrypting (S102aa) the dispenser certificate (506) using a certificate key; and
(j) - comparing (S102ac) one or more elements of the authentication data with corresponding elements of the decrypted dispenser certificate, and wherein
(k) verifying the dispenser certificate (506) fails if at least one or more elements of the authentication

data does not match the corresponding element of the decrypted dispenser certificate,

(l) - updating (S103) the hearing device configuration based on the configuration package (402) if the update criterion is fulfilled."

IV. Claim 1 of **auxiliary request A1** differs from claim 1 of the main request in that it further comprises, between features (h) and (i), the following feature (board's feature labelling):

(m) "wherein determining (S102) if the update criterion is fulfilled comprises verifying (S102a) the dispenser certificate (506), wherein the update criterion is not fulfilled if verifying the dispenser certificate (506) fails,".

V. Claim 1 of **auxiliary request A2** differs from claim 1 of auxiliary request A1 in that it further comprises, between features (k) and (l), the following feature (board's feature labelling):

(n) "wherein comparing (S102ac) one or more elements of the authentication data with corresponding elements of the dispenser certificate (506) comprises comparing one or more elements of the authentication data received in plain text with corresponding elements of the decrypted dispenser certificate;".

VI. Claim 1 of **auxiliary request A3** differs from claim 1 of auxiliary request A2 in that it further comprises, between features (l) and (n), the following feature (board's feature labelling):

(o) "and
- determining (S102ad) if the fitting device (2) and/or the dispenser is blacklisted, and wherein verifying the dispenser certificate (506) fails if the fitting device and/or the dispenser is blacklisted; and".

VII. Claim 1 of **auxiliary request A4** differs from claim 1 of auxiliary request A3 in that it further comprises, at the end, the following feature (board's feature labelling):

(p) ", wherein the configuration package (402) comprises a configuration data integrity indicator, and wherein updating (S103) the hearing device configuration comprises verifying (S103c) the configuration data integrity indicator based on the configuration package (402), and terminating the update of the hearing device configuration based on the configuration package (402) if the verification of the configuration data integrity indicator fails".

Reasons for the Decision

1. *Opposed patent - technical background*

1.1 The opposed patent relates to a method for updating the configuration of a hearing device. The patent describes a hearing system (1) comprising a server device (4), a fitting device (2), a user accessory device (10) and the hearing device (8) itself (see Figure 1, reproduced below).

1.2 The invention underlying the opposed patent addresses the problem of securing the configuration-update process to prevent unauthorised parties from modifying the hearing-device settings, which could potentially harm the user (e.g. by setting excessive amplification levels).

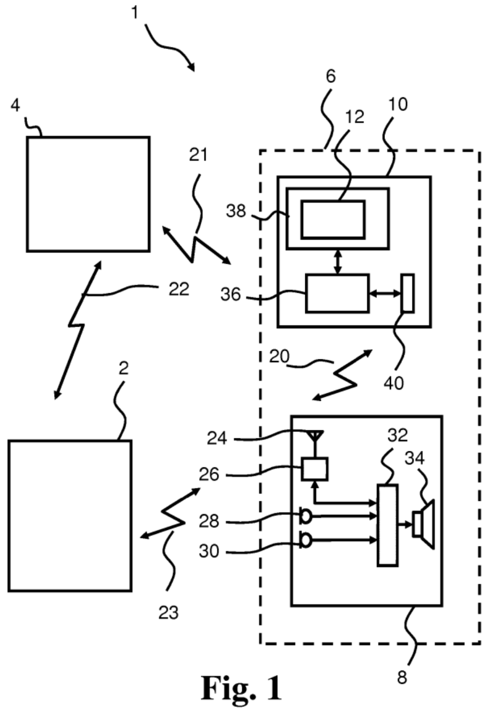

Fig. 1

The opposed patent proposes a solution wherein the hearing device receives a "configuration package" (containing the new settings) and a "configuration authentication package". The latter contains a "dispenser certificate" and "authentication data". As a part of a data verification process, the hearing device decrypts the dispenser certificate and compares elements of the authentication data with corresponding elements of the dispenser certificate. The configuration update is performed only if an update criterion based on this verification process is fulfilled.

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

2.1 In relation to claim 1 of the **main request**, the opposition division considered prior-art document **D1** to be a suitable starting point for the assessment of inventive step in Reasons 14.2 of the appealed decision. The parties did not dispute this and neither does the board.

Moreover, while Reasons 14.2.1 of the appealed decision found that D1 did not disclose features (f) and (h) to (k), the board will adopt, *arguendo*, the proprietor's view that **features (e) to (l)** are not disclosed in D1.

2.2 The parties differed in their views regarding the technical effect associated with the features distinguishing the claimed subject-matter from D1:

2.2.1 The technical effect considered by the opponent resided initially in an "efficient" implementation of a "secure update mechanism of the hearing device". Later, during the oral proceedings before the board, the opponent considered that there was no technical effect that was credibly achieved.

2.2.2 The proprietor, referencing paragraphs [0003], [0013] and [0014] of the opposed patent (corresponding to page 1, lines 17 to 22 and page 3, line 30 to page 4, line 25 of the application as filed), asserted that features (e) to (l) achieved the provision of a *secure* configuration update of a hearing device. The board notes that the opposition division accepted this view without detailed justification, as can be gathered from Reasons 14.2.2 of the appealed decision.

During the oral proceedings before the board, the proprietor argued that all the distinguishing features together "produced a synergistic effect" and had "a very specifically intertwined technical meaning". It further submitted that the features were interrelated, relying on the receipt of the "configuration package" alongside the "configuration authentication package", which includes "authentication data" and an encrypted "dispenser certificate". The proprietor emphasised that the data verification according to the claimed method ensured that the data was not tampered with and that this was done not by conventional means, but by decrypting the certificate using a certificate key derived *only* by the hearing device and subsequently performing the claimed comparison. As an alternative, the proprietor also considered that the distinguishing features contributed to a *control* of the updating of the hearing-device configuration.

2.3 However, the board finds that claim 1 is formulated broadly. For example, regarding feature (l), claim 1 is silent as to what happens if the "update criterion" is not fulfilled, i.e. as to the necessary constraints to strictly prevent an unauthorised configuration update. Furthermore, claim 1 is silent as to where the "packages" referred to in feature (e) originate from and where the "certificate key" mentioned in feature (i) comes from. Furthermore, this claim leaves it entirely open whether any actual security effect is achieved at all, let alone whether it relates to authorisation, authentication, data integrity, non-repudiation, confidentiality or a combination thereof. Moreover, claim 1 as granted uses undefined terminology (e.g. "authentication data", "comparing" and "dispenser certificate") rather than specific definitions regarding cryptographic security.

During the oral proceedings before the board, the proprietor argued that a comparison of the respective data elements to see if they "match" requires checking whether those elements are identical to each other, rather than, for instance, merely checking if metadata is present. However, the board agrees with the opponent that claim 1 is silent as to a definition of the matching criterion and that both the terms "match" and "element" are broad and elusive. A "match" does not necessarily require a bit-by-bit identity; it could merely mean that the data have a predetermined correlation, such as the same length or the same data structure. Similarly, the term "element" is broad and could simply refer to a *type* of data, without requiring a comparison of the actual substantive *content*. This means in particular that the claimed method is silent as to the necessary constraints to guarantee a minimum level of security or to strictly prevent unauthorised updates. The board further notes that the proprietor heavily relied on the patent description to read limitations into the claim that are not present in its wording. While the board, in accordance with the finding of the Enlarged Board of Appeal in **G 1/24** (see its Headnote and Reasons 12 and 18), has consulted and referred to the patent description and drawings to define the skilled reader from whose perspective the claims are to be interpreted (see e.g. **T 1465/23**, Reasons 2.4, and **T 1924/20**, Reasons 2.7), it has become a widely accepted principle that the legally relevant subject-matter of a patent is defined by its claims as the starting point and decisive basis for claim interpretation and that limitations taken solely from the description cannot be read into a claim to restrict the claimed subject-matter (see e.g. **T 2027/23**).

Regarding the proprietor's alternative formulation that the distinguishing features contribute to a "control" of the updating, the board finds this formulation to be exceedingly broad and thus invalid from the outset. Updating a hearing device based on any condition — or indeed, merely *scheduling* an update — constitutes a form of "control". Such a control can be exerted without any form of security. Consequently, the highly specific cryptographic steps recited in features (e) to (l) cannot be seen as being directly and causally linked to such a generic concept of "control". Rather, analogous to the situation addressed by this board in decision **T 1465/23** (see Reasons 2.3 and 2.6 to 2.8), the claimed features merely amount to "isolated islands of cryptography" that fail to functionally interact to provide a credible, systemic security effect over the whole scope of claim 1.

In sum, the board is not persuaded that the alleged technical effects of "secure update" or "control" are directly and causally related to the technical features of the claimed invention and must be rejected offhand.

2.4 Nevertheless, even if a technical effect were acknowledged — for instance by assuming that these "isolated islands of cryptography" provide at least some partial security benefit — the subject-matter of claim 1 would still lack an inventive step. In this regard, the board notes that restricting the objective technical problem to an *attempt to at least partly implement* the authentication scheme aligns with the view that was essentially common ground between the parties during the oral proceedings before the board. In particular, the opponent correctly observed that the claimed verification steps do not establish a complete security chain, but merely represent "puzzle pieces" of an overall authentication process. The proprietor implicitly concurred with this assessment, conceding that the claimed method represents only one "stage" of a "complete security architecture" involving other devices and keying materials that are not defined in claim 1 and conceding that the configuration update is secured only "*to the extent that the checks are performed*". Consequently, the board considers that formulating the objective technical problem as a partial implementation of D1's authentication scheme appropriately captures the converging views expressed by the parties during the oral proceedings before it.

2.5 Therefore, the board formulates the objective technical problem *arguendo* as "how to attempt to at least partly implement an authentication scheme as indicated in D1". This formulation is mainly based on the disclosure of D1, which explicitly mentions "authentication schemes" in paragraph [0141], "unauthorized access" prevention in paragraph [0139] and "misuse protection" in paragraph [0090].

2.6 However, the skilled person from the field of secure data transmission, tasked with solving this objective technical problem starting from D1, would have arrived at the claimed features based on their common general knowledge for the following reasons:

2.6.1 Feature (e) - "configuration package":

In any authenticated transmission, it is standard practice that one cannot simply send the data alone. One must send the "data", i.e. the "configuration package" such as the one in accordance with feature (e), *and* the "proof" required for its authentication, namely its "security credentials" such as a signature or a certificate like the one mentioned in feature (e).

During the oral proceedings before the board, the proprietor argued that comparing two parts of the same "configuration authentication package" as per feature (j), where one part is encrypted and is a certificate, was non-standard and not found in the prior art. However, the board finds that the logical receipt of a "payload" alongside its "security credentials" is an inherent and well-known requirement of any authenticated transfer. Whether the data and the proof are transmitted via two separate streams or bundled together into a single file (a "container") as defined in claim 1 is merely a routine design choice. Grouping them into the same package represents a straightforward implementation detail with known benefits (e.g. easier data processing) and drawbacks (e.g. higher vulnerability to eavesdropping) that provides no inventive contribution.

2.6.2 Feature (f) - "configuration authentication package":

To verify a digital signature or authenticate a source, the receiver typically requires the sender's public key. To trust that public key, it was and still is part of the skilled person's common general knowledge (as evidenced for instance by **D3**) that this public key must be wrapped in a certificate issued by a trusted authority ("trusted third party", e.g. the manufacturer or a hearing-aid acoustician). Therefore, as part of their efforts to solve the problem posed, the skilled person would have had to include the "dispenser certificate" in the authenticated transmission mentioned in point 2.6.1 above to allow for data verification.

The proprietor acknowledged orally that D1 provided a hint towards unauthorised access control, checksums and hashes, but argued that starting from D1 alone the skilled person was not taught to implement the specific features of claim 1 and specifically lacked any prompt towards a "dispenser certificate" as per feature (f). The board notes, however, that the skilled person would have immediately understood that authenticating the source (the "dispenser" or "fitting device" in the claim's terminology) is the explicit goal of the authentication scheme mentioned in paragraph [0141] of D1 and that the use of a certificate like the one mentioned in feature (f) is a standard, routine way to achieve this.

2.6.3 Features (g) and (l) - "update criterion":

Document D1 instructs the use of an "authentication scheme" as an example of a "secure connection" in paragraph [0141]. The sole purpose of such an authentication scheme is to act as a sort of gatekeeper. As noted in point 2.3 above, claim 1 broadly requires updating the configuration if the "update criterion" is fulfilled, and is silent as to what happens if the criterion is not fulfilled. However, the skilled person implementing the authentication scheme of D1 would have inherently implemented a strict logic based on their common general knowledge: the process proceeds with editing the operability data ("update") as set out in paragraph [0141] of D1 if the authorised-access check mentioned in paragraph [0139] of D1 passes and it is blocked if this check fails. Because this routine implementation of D1 inherently includes the action of updating when the check passes, they would have inevitably arrived at a method falling within the broad meaning of feature (l). Making the configuration update conditional on the result of the data verification according to the claimed method does therefore not require an inventive step: it is merely the logical consequence of implementing the teaching of D1.

2.6.4 Features (h) and (i) - authentication logic:

A data verification step such as the one in accordance with feature (h) typically requires mathematical operations. It goes without saying that one cannot "verify" a digital certificate merely by inspection. Standard verification typically involves, as orally explained by the opponent, validating the digital signature of the certificate's issuer. The opponent is right that the skilled person would have known, based on their common general knowledge, that validating a digital signature technically involves using a key to "decrypt" the string that represents the digital signature. Thus, the step of decrypting the "dispenser certificate" using a pre-stored and valid "certificate key" as per feature (i) describes the standard mechanics of data verification.

During the oral proceedings before the board, the proprietor argued that there are many conventional security protocols that are part of the skilled person's common general knowledge, such as the challenge-response protocol or verifying the signature of messages, and questioned why the skilled person would have selected precisely the intricate steps claimed. The proprietor emphasised that nothing in D1 would have prompted the skilled person to adopt a solution falling under the claim. However, the board finds that the proprietor's argument — that the claim implies a specific, unique protocol (encrypting the "dispenser certificate") distinct from standard public-key infrastructure — is not persuasive. Such an implementation would have merely represented an arbitrary choice among equally likely known alternatives for authenticating a transmission, providing no inventive contribution.

2.6.5 Feature (j) - "comparing":

As the opponent orally explained, an "authentication" such as the one mentioned in claim 1 is fundamentally a comparison operation (comparing "what is *presented*" against "what is *expected*"). The claimed step of comparing "elements" as per feature (j) covers routine consistency checks performed in standard security protocols (e.g. checking if the sender ID in the packet header matches the subject name in the certificate) that are inherent to an authenticated transmission such as the one referred to in point 2.6.1 above. Therefore, the opponent is right that one cannot implement a working authentication scheme as mentioned in D1 without comparing data.

During the oral proceedings before the board, the proprietor challenged the opponent to explain how an attacker could tamper with a specific element of the decrypted "dispenser certificate" and tamper in parallel with the corresponding element of the "authentication data" to make the comparison according to feature (j) pass, concluding that such a tampering was impossible. The board does not accept this argument. As pointed out by the opponent, this conclusion ignores the vulnerability of the claimed method to replay attacks using validly intercepted configuration packages. Crucially, while feature (e) requires the provision of both a "configuration package" and a "configuration authentication package", claim 1 fails to require any cryptographic binding between the two. For instance, claim 1 does not specify that the "authentication data" comprised by the latter "package" in accordance with feature (f) is calculated over the specific configuration data contained within the former package. Without this indispensable cryptographic link, an attacker can simply execute a replay attack by pairing validly intercepted credentials with maliciously altered configuration data. Thus, the comparison in accordance with feature (j) is, as the opponent explained orally, merely a standard consistency check.

2.6.6 Feature (k) - failure condition:

This feature states that verification fails if "elements" do not "match". As established in point 2.3 above, the terms "elements" and "match" are broad. In particular, and contrary to what was stated by the proprietor during the oral proceedings before the board, the term "match" does not necessarily require that a comparison of substantive "contents" is made. Because of this breadth, feature (k) could very well relate to a check whether the decrypted "dispenser certificate" and the "authentication data" have the same length or data type, which is a standard verification process for any transmission, such as the one mentioned in point 2.6.1 above. Furthermore, the technical process of any "verification" inherently relies on establishing a predefined correspondence between data items: if such a correspondence is absent, the data verification necessarily fails. Consequently, this feature merely renders explicit a logical necessity and provides no inventive contribution.

2.7 Hence, features (e) to (l) would have represented at most a routine implementation of the "authentication schemes" found in D1 for the skilled person using their common general knowledge.

2.8 Consequently, the subject-matter of claim 1 as granted does not involve an inventive step (Article 56 EPC). Therefore, contrary to the finding of the opposition division in Reasons 14.1 of the appealed decision, the ground for opposition under Article 100(a) in conjunction with Article 56 EPC prejudices the maintenance of the patent as granted.

3. *Request for remittal of the case*

3.1 The proprietor requested that the case be remitted to the opposition division if the main request was found to be not allowable (cf. point II above), arguing that there was no decision on the auxiliary requests from the opposition division and that, therefore, the board lacked competence to judge them.

3.2 Pursuant to Article 11 RPBA, the board shall not remit a case for further prosecution to the department whose decision was appealed unless "special reasons" present themselves for doing so.

3.3 The board sees no such "special reasons" in the present case. The fact that the opposition division did not decide on the auxiliary requests because it allowed the main request is a standard procedural situation in appeal proceedings. Under Article 111(1) EPC (second sentence, first alternative), the board is fully competent to review the entire case, including amendments filed during these proceedings. To accept the proprietor's argument would effectively amount to granting a right to two instances for every amendment or aspect of the case. Yet, such a right is not enshrined in the EPC and would be contrary to the principle of procedural economy.

3.4 Consequently, the request for remittal has been refused.

4. *Auxiliary requests A1 to A4: claim 1 - inventive step*

The amendments underlying claim 1 of **auxiliary requests A1 to A4** do not overcome the objection regarding lack of inventive step identified for claim 1 of the main request. The reasons for this are as follows.

4.1 Auxiliary request A1

4.1.1 Claim 1 of auxiliary request A1 adds **feature (m)**, which states that the "update criterion" is not fulfilled if verifying the "dispenser certificate" fails.

4.1.2 During the oral proceedings before the board, the proprietor argued that the distinguishing features had to be considered as a whole and not in a piecemeal fashion, taken out of context. The proprietor submitted that, since the "update criterion" was not fulfilled if verifying the "dispenser certificate" fails as expressed in feature (m), claim 1 now specified very clearly how the data verification was performed and that one did not proceed to the configuration update because the "update criterion" was not fulfilled.
The board notes first that the latter assertion — i.e. that the method does not proceed to the update if the "update criterion" is not fulfilled — is still not explicitly reflected in claim 1. However, even assuming

that feature (m) successfully addresses the deficiency identified in point 2.3 above - i.e. that the claim does not specify what happens if the "update criterion" is not fulfilled - by explicitly linking a failed verification of the "dispenser certificate" to an unfulfilled "update criterion", this added feature cannot confer an inventive step. Applying, *arguendo*, the same objective technical problem as formulated for the main request in point 2.5 above, the skilled person tasked with implementing the authentication scheme of D1 in accordance with that objective technical problem would have designed, without inventive effort, the system at hand such that a failed verification simply results in the authentication criterion not being met. In other words, a security gate that considers its criterion to be fulfilled regardless of whether the correct key is presented is not a functional security gate. Therefore, explicitly formulating this "failed verification = unfulfilled criterion" logic is not an inventive contribution, but merely the direct and obvious technical consequence of implementing any standard authentication scheme as instructed by D1. The proprietor's argument that feature (m) clarifies the "control" aspect of its alternative objective technical problem (cf. the last paragraph of point 2.2.2 above) is noted, but it does not alter the fact that a sort of "*fail = stop*" logic is an inherent and well-known requirement of any working authentication scheme such as the one requested by D1.

4.1.3 The proprietor also argued that proof is required regarding the skilled person's common general knowledge.

However, this argument was presented in a boilerplate manner and the proprietor failed to specify which exact parts of that common general knowledge were being contested. The board has no reason to doubt or contest any of the elements of the skilled person's common general knowledge used in the obviousness analysis for the main request and the auxiliary requests.

4.1.4 Therefore, the addition of feature (m) does not confer an inventive step as regards claim 1 of auxiliary request A1.

4.2 Auxiliary request A2

4.2.1 Claim 1 of auxiliary request A2 adds **feature (n)**, i.e. requiring the comparison of "plaintext authentication data" with elements of the "decrypted dispenser certificate".

4.2.2 This feature, however, describes a standard consistency check. In security protocols, the receiver routinely compares the sender identity in the message header (i.e. the "plaintext authentication data") with the subject identity inside the "certificate" (the decrypted certificate elements) to prevent spoofing.

4.2.3 The proprietor's argument that comparing plaintext data is a specific, non-obvious implementation detail is unconvincing, as this is a necessary routine step to ensure that the certificate actually belongs to the current session or sender.

4.2.4 The proprietor emphasised that the relevant issue was not whether the whole message was sent in plaintext or encrypted, but whether parts of it were encrypted. The proprietor stated that there was a dichotomy in that, within the same "configuration authentication package", it had been decided that *one* part is plaintext and *another* part was encrypted. The proprietor emphasised that the skilled person could have envisaged doing it the other way around and that there was no reason why they would have arrived at the specific choice set out in feature (n).

However, the board finds that this represents a mere choice between equally likely design alternatives, which cannot contribute to an inventive step.

4.2.5 As a result, the addition of feature (n) cannot contribute to inventive step, either.

4.3 Auxiliary request A3

4.3.1 Claim 1 of auxiliary request A3 adds **feature (o)**, specifying that "verifying" comprises determining if the dispenser is "blacklisted".

4.3.2 For this auxiliary request, the board considers the objective technical problem to be the same as for the main request (cf. point 2.5 above), but with the term "implement" understood to also cover energy-efficiency considerations. As a result, the board phrases the objective technical problem for auxiliary request A3 as: "*how to adapt the system in D1 such that its authentication scheme is at least partly implemented in an energy-efficient way?*".

4.3.3 Concerning obviousness, the opponent is right that there is no synergy between the distinguishing features of the main request and that of auxiliary request A3, i.e. feature (o). Moreover, the board finds that the skilled person would have been familiar with "blacklisting" as per feature (o) based on their common general knowledge. In fact, establishing and using an access control list in the form of a "whitelist" or "blacklist" constitutes the most simple and obvious way of ensuring secure access to certain data or entities.

4.3.4 During the oral proceedings before the board, the proprietor argued that paragraph [0141] of D1 states that a secure data connection is accomplished using data encryption, etc. It emphasised that "blacklisting" had nothing to do with the connection itself, but was rather about verifying whether the "certificate" of the "dispenser" or "fitting device" had been corrupted, figuring this out via a "blacklist" on the server. In the proprietor's view, the skilled person would have had no reason to arrive at the claimed solution because feature (o) was not about securing a data connection based on authentication schemes.

4.3.5 However, in the board's opinion, paragraph [0141] of D1 uses the term "secure connection" in a broad sense. This is apparent from the examples enumerated in that paragraph, which range from "data encryption" and "authentication" to the "acknowledgement of a successful transmission". In this context, the board finds that "blacklisting" (e.g. using a kind of certificate-revocation lists) is a fundamental component of standard public-key infrastructure. Furthermore, for a battery-constrained device like a hearing aid (as in D1), it would have been obvious to perform a computationally "cheap" check (e.g. a database lookup for a "blacklist") before performing an "expensive" check (e.g. cryptographic decryption). Moreover, paragraph [0090] of D1 also explicitly refers to "misuse" prevention. This paragraph reads as follows:

> "*[...] a misuse protection is provided. Making said data set misuse-proof can be accomplished, e.g., by encryption and/or by using a checksum/hash with a secret secure checksum/hash generating algorithm, and/or by using authentication schemes between fitting system and hearing device, and/or any other applicable cryptographic method.*"

The skilled person in the field of data security would be well aware that such a "misuse protection" typically encompasses "blacklisting". The same applies to the expression "*prevent unauthorized access*" used in paragraph [0139] of D1.

4.3.6 The proprietor argued that the only mention in D1 of "security schemes" was in paragraph [0141] and that one should therefore concentrate solely on this paragraph when addressing the problem to be solved.

This is not convincing. Given the broad way in which the term "secure connection" is used in D1, the skilled person would have understood that one of equally likely ways in which the objective technical problem formulated in point 4.3.2 above can be solved is by focusing on a "misuse" prevention as per paragraph [0090] or preventing "unauthorized access" as per paragraph [0139] of D1.

4.3.7 Thus, also the application of feature (o) to the system of D1 is an obvious measure to the skilled person.

4.4 Auxiliary request A4

4.4.1 Claim 1 of auxiliary request A4 adds **feature (p)**, i.e. requiring the verification of a so-called "configuration data integrity indicator".

4.4.2 The board considers the objective technical problem in view of feature (p) to be: "*how to adapt the system of D1 such that an integrity check is practically implemented?*".

4.4.3 Concerning obviousness, the opponent rightly noted, similar to the analysis for feature (o) set out in point 4.3.3 above, that there is no synergy between the distinguishing features of the main request and that of auxiliary request A4, and that feature (p) is, as a result, a mere "add-on". Moreover, the board considers that paragraphs [0113], [0139] and [0141] of D1 explicitly suggest using "an integrity check", "hashes", "checksums" or "data packet identifiers" to ensure data integrity. A "configuration data integrity indicator" in accordance with feature (p) is merely a generic term for a "checksum" or "hash". Based on their common general knowledge, the skilled person would thus have considered it to be a universal engineering practice to verify a checksum before installing a configuration update to prevent update errors.

4.4.4 The proprietor's argument that feature (p) provides a synergistic security effect is not accepted: the opponent is right that the "configuration data integrity indicator" mentioned in feature (p) is merely a stand-alone check for transmission errors or data corruption, as already suggested by D1.

4.4.5 Moreover, the proprietor's argument that the paragraphs [0113], [0139] and [0141] of D1 describe unrelated embodiments could not sway the board, either. The skilled person would have immediately understood that the term "integrity check" mentioned in paragraph [0113] of D1 and the expression "*prevent unauthorized access*" used in paragraph [0139] of D1 are related to each other and that both are related to the "secure connection" examples enumerated in paragraph [0141] of D1, such as the "acknowledgement of a successful transmission" recited therein.

4.4.6 Consequently, feature (p) can likewise not contribute to inventive step.

4.5 In conclusion, none of auxiliary requests 1 to 4 meets the requirement of Article 56 EPC.

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:

Beschwerdekammern des Europäischen Patentamts
Boards of Appeal of the European Patent Office
Chambres de recours de l'Office européen des brevets

B. Brückner K. Bengi-Akyürek

Decision electronically authenticated