BESCHWERDEKAMMERN DES EUROPÄISCHEN PATENTAMTS

BOARDS OF APPEAL OF THE EUROPEAN PATENT OFFICE

CHAMBRES DE RECOURS DE L'OFFICE EUROPEEN 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 15 October 2010

Case Number: T 0152/07 - 3.5.06

Application Number: 99908851.1

Publication Number: 1058872

IPC: G06F 1/00

Language of the proceedings: EN

Title of invention:
Method, arrangement and apparatus for authentication through a communications network

Patentee:
Telefonaktiebolaget LM Ericsson (publ)

Opponent:
SWISSCOM AG
GIESECKE & DEVRIENT GmbH

Headword:
-

Relevant legal provisions:
-

Relevant legal provisions (EPC 1973):
EPC Art. 56
RPBA Art. 13(1), 12(1)(3)

Keyword:
"Basis of decisions - opportunity to comment (yes)"
"Late filed response to appeal admitted"
"Inventive step (no)"

Decisions cited:
G 0009/92, G 0004/93

Catchword:
-

Europäisches Patentamt | European Patent Office | Office européen des brevets

Beschwerdekammern | Boards of Appeal | Chambres de recours

Case Number: T 0152/07 - 3.5.06

D E C I S I O N
of the Technical Board of Appeal 3.5.06
of 15 October 2010

Appellant: (Patent Proprietor)	Telefonaktiebolaget LM Ericsson (publ) S-164 83 Stockholm (SE)
Representative:	Akerman, Marten Lennart Ericsson AB Patent Unit Mobile Platforms S-221 83 Lund (SE)
Respondent 1: (Opponent 1)	SWISSCOM AG Viktoriastraße 21 CH-3050 Bern (CH)
Representative:	Saam, Christophe Patents & Technology Surveys SA Terreaux 7 Case Postale 2848 CH-2001 Neuchâtel (CH)
Respondent 2: (Opponent 2)	GIESECKE & DEVRIENT GmbH Prinzregentenstr. 159 D-81677 München (DE)
Representative:	-
Decision under appeal:	**Interlocutory decision of the Opposition Division of the European Patent Office posted 15 November 2006 concerning maintenance of the European patent No. 1058872 in amended form.**

Composition of the Board:

Chairman: D. H. Rees
Members: A. Teale
M-B. Tardo-Dino

Summary of Facts and Submissions

I. This is an appeal by the patent proprietor against the interlocutory decision by the opposition division that, account being taken of the amendments made by the proprietor during the opposition proceedings according to the proprietor's then sixth auxiliary request, European patent No. 1 058 872 and the invention to which it related met the requirements of the EPC. Oppositions had been filed by opponents 1 and 2.

II. The reasons for the appealed decision stated *inter alia* that the subject-matter of claim 1 according to the proprietor's then first auxiliary request lacked inventive step, Article 56 EPC 1973, in view of the following prior art document:

D1: US 5 668 876 A

and the reference in D1 to the A3 algorithm of the GSM 03.20 standard. The subject-matter of claim 1 according to the proprietor's then second and third auxiliary requests was found to lack inventive step, Article 56 EPC 1973, in view of D1 and the following prior art document:

D2: Recommendation GSM 03.20 "Security-related Network Functions", version 3.3.2, release date February 1992, ETSI (European Telecommunications Standards Institute), B.P.152.F - 06561 Valbonne Cedex, France, 48 pages.

The decision also referred to the following prior art documents, amongst others:

D3: GSM 11.11 version 3.16.0, "Specifications of the SIM-ME Interface", ETSI PT12, July 1994, 132 pages.

D4: Document GSM 173/87, "Functional splitting of the mobile station in mobile equipment and subscriber identity module", CEPT CCH/GSM-TE SEG, Bonn, 21 to 23 September 1987, 9 pages.

III. A notice of appeal and appeal fee were received from the proprietor on 25 January 2007, a statement of grounds of appeal being received from the proprietor on 16 March 2007. With the statement of grounds of appeal the appellant (proprietor) filed amended claims according to a main and first and second auxiliary requests. The appellant requested that the appealed decision be set aside and that the patent be maintained on the basis of the claims according to the main and first and second auxiliary requests, in that order. The appellant also made an auxiliary request for oral proceedings.

IV. In the statement of grounds of appeal the appellant argued essentially as follows.

Main request

The objective problem starting from D1 was to provide *inter alia* a method for authenticating a user to an application, which was of low complexity and inexpensive. D1 did not render the subject-matter of the independent claims obvious. D1 mentioned the

algorithm unit calculating a response code using optionally a secret key provided by the supplier of the personal unit. In contrast, claim 1 set out the step of authenticating the user to an application comprising utilizing secret information of the second communications network stored on a SIM. D1 did not make any use of the second communications network apart from transporting the authentication information. In D1 the secret information stored on the SIM was provided by the operator, not the cell phone manufacturer. Moreover a "cellular phone" did not even have to include a SIM card. Indeed D1 did not mention a SIM card. D1 only gave the A3 algorithm of the GSM 03.20 standard as an example of a possible algorithm. It would not have been obvious for the skilled person starting from D1 to use the secret code on the SIM for authenticating a user to an application. The subject-matter of claim 1 differed from the disclosure of D1 in including the step of utilizing secret information of the second communications network stored on a SIM or information provided in the HLR and/or VLR database of the second communications network when authenticating a user to an application. The advantage of this difference was that the implementation of the invention was less complex, required no or significantly less additional hardware and software and was consequently less expensive to build and maintain. An authentication centre, as disclosed in D1, was not required, and there was no need to modify the mobile station, contrary to the case of the personal unit of D1.

First auxiliary request

The reference in D1 to GSM 03.20 did not disclose the use of the HLR and/or VLR for authenticating a user to

an application. The feature in claim 1 relating to the HLR and/or VLR databases had to be considered in the context of the claim as a whole. None of the available prior art taught to utilize secret information of the second communications network stored on a SIM and information provided in the HLR and/or VLR database of the second communications network for authenticating the user to an application. Doing so increased security because the authentication of a user to an application relied on information which was split between more than one location (i.e. on the SIM card and in the HLR and/or VLR database). Neither this problem nor its solution was known from any of the cited prior art references.

Second auxiliary request

D1 did not disclose all the functional features of the MS PAD (Mobile Station Personal Authentication Device). The invention made use of a cellular phone comprising a PAD to control the authentication operation which utilized secret information of the second communications network stored on a SIM or information provided in the HLR and/or VLR database of the second communications network.

V. In a communication dated 21 March 2007 the board informed respondents 1 and 2 (opponents 1 and 2, respectively) of the grounds of appeal and stated that any reply was to be filed within four months of the notification, i.e. by 31 July 2007, Rule 78 (2) EPC 1973.

VI. In two telefaxes, both dated and received on 24 July 2007, respondent 2 requested an extension of the four month time limit by a further two months to allow further discussions between respondent 2 and its representative.

VII. In a communication dated 25 July 2007 the board refused respondent 2's request for a time extension essentially because the reasons provided by respondent 2 were not considered sufficient to prove that this was an exceptional case, Article 10a(5) RPBA (Rules of Procedure of the Boards of Appeal of the EPO)(in the version valid at that time).

VIII. In a letter dated 27 July 2007 and received on the same day respondent 2 requested that the appeal be dismissed and also made an auxiliary request for oral proceedings.

IX. In a letter dated 3 September 2007 and received on 4 September 2007 respondent 2 requested that the patent be revoked and reiterated the auxiliary request for oral proceedings. Respondent 2 also argued essentially as follows.

Main request

The reference in D1 (column 4, line 24 onwards) to GSM 03.20 and its A3 authentication algorithm would have prompted the skilled person to use the SIM card, as was usual in this authentication algorithm. D2 stated (page 42, point A3.2.2) that the A3 algorithm was contained in the SIM card and in the HLR or VLR on the network side. Hence the reference in D1 to GSM 03.20 would have prompted the skilled person to use the A3 algorithm for authentication, this algorithm

using a secret in the SIM card and in the network. Regarding the secret key K_i in the SIM card, reference was also made to D4 (page 3, lines 8 to 9) which stated that the authentication key K_i was stored in the SIM card and was unreadable from outside it. Hence on the user side the A3 algorithm was carried out in the SIM card, as also stated in D2. The GSM A3 algorithm was the only concrete example of a suitable algorithm disclosed in D1 and was moreover an obvious choice for the skilled person seeking the least complex and most economical solution. If the GSM network were to be used as a second communication network, as set out in D1 (column 3, lines 44 to 50), then it would be simplest and most economical to use the known and widely-used authentication algorithm already present. According to this algorithm, as set out in the characterizing part of the claims, secret information (K_i) on the chip card and secret information in the HLR or VLR data base was used to carry out authentication. By choosing this authentication method no further measures would have been required, and the existing hardware and software infrastructure could have been used. The same argumentation applied to claims 1, 11 and 16.

First auxiliary request

This request differed from the main request in that a secret in the SIM card and information from the HLR or VLR was used for authentication. As stated in D2 and D4, and as would have been apparent to the skilled person, in a symmetrical algorithm like the A3 algorithm the secret key must be known to both sides, i.e. both the SIM card and the network (meaning the HLR or VLR, depending on whether the mobile station was registered with its own or another network.) Hence claims 1, 11

and 16 lacked inventive step in view of D1 and common general knowledge (as exemplified by D2 and D4).

Second auxiliary request

According to this request, in addition to the alternatives set out in the main and first auxiliary requests, authentication operations were controlled by means in the mobile station. Since however the algorithm was stored in the SIM card (see D4) and authentication signals had to be exchanged with the network, it would have been inevitable that parts of the mobile station between the SIM card and the network would have controlled communication between the SIM card and the network. Claims 1, 11 and 16 consequently lacked inventive step in view of D1 combined with D2 and, if need be, D4.

X. No substantive response to the appeal was received from respondent 1.

XI. The board issued a summons to oral proceedings, setting out its provisional opinion on the appeal in an annex to the summons. The board questioned the admissibility of respondent 2's request for revocation of the patent, since this appeared to result in a situation of *reformatio in peius* for the appellant. It seemed that recommendation GSM 03.20 (set out in D2), the specifications of the SIM-ME interface (set out in D3) and the functional splitting of the GSM mobile station (set out in D4) were common general knowledge at the priority date. The subject-matter of the independent claims according to the appellant's main and first and second auxiliary requests seemed to lack inventive step in view of D1 and common general knowledge (as

exemplified by D2, D3 and D4), the GSM A3 authentication algorithm falling within the terms of the characterizing parts of the independent claims. The board also expressed doubts concerning clarity (Article 84 EPC 1973) and sufficiency of disclosure (Article 83 EPC 1973).

XII. In a letter dated 5 July 2010 respondent 1 stated that he did not intend to be present at the oral proceedings and instead requested that a decision be taken according to the state of the file. Respondent 1 did not comment on the substance of the case.

XIII. In a letter dated 18 August 2010 the appellant stated that he would not attend the oral proceedings and wished to be informed of the board's decision. The appellant did not comment on the substance of the case.

XIV. The board issued a communication dated 25 August 2010 to the parties stating that "Since neither the appellant nor opponent 1 intends to be present at the oral proceedings, and in view of the board’s preliminary opinion on the appeal set out in the annex to the summons to oral proceedings, the board would like to enquire whether opponent 2 still maintains his auxiliary request for oral proceedings. If this auxiliary request were to be withdrawn then the board would cancel the oral proceedings and issue a decision."

XV. In a telefax dated 23 August 2010 respondent 2 stated that it withdrew its auxiliary request for oral proceedings if the board were to decide as set out in its preliminary opinion in the annex to the summons to

oral proceedings. Respondent 2 did not however comment on the substance of the case.

XVI. In a communication to the parties dated 27 August 2010 the board announced that the oral proceedings had been cancelled.

XVII. Claim 1 according to the appellant's main request reads as follows:

"A method for authenticating a user (22) to an application (45), the application (45) being available to the user (22) through a first communications network, the method comprising: establishing a connection between the application (45) and a user interface (16) through the first communications network so as to enable a user (22) to access the application (45); establishing a connection between the application (45), which may connect to a database (46) to which a mobile station (1, 2) is registered, and the mobile station (1, 2) through a second communications network; authenticating the user (22) to the application (45) by means of the mobile station (1, 2) communicating with the application (45) through the second communications network characterized in that the step of authenticating the user comprises utilizing secret information of the second communications network stored on a SIM (34) or information provided in HLR (9) and/or VLR (8) database of the second communications network."

XVIII. Claim 1 according to the appellant's first auxiliary request reads as follows:

"A method for authenticating a user (22) to an application (45), the application (45) being available to the user (22) through a first communications network, the method comprising: establishing a connection between the application (45) and a user interface (16) through the first communications network so as to enable a user (22) to access the application (45); establishing a connection between the application (45), which may connect to a database (46) to which a mobile station (1, 2) is registered, and the mobile station (1, 2) through a second communications network; authenticating the user (22) to the application (45) by means of the mobile station (1, 2) communicating with the application (45) through the second communications network characterized in that the step of authenticating the user comprises utilizing secret information of the second communications network stored on a SIM (34) and information provided in HLR (9) and/or VLR (8) database of the second communications network."

XIX. Claim 1 according to the appellant's second auxiliary request reads as follows:

"A method for authenticating a user (22) to an application (45), the application (45) being available to the user (22) through a first communications network, the method comprising: establishing a connection between the application (45) and a user interface (16) through the first communications network so as to enable a user (22) to access the application (45); establishing a connection between the application (45), which may connect to a database (46) to which a mobile station (1, 2) is registered, and the mobile

station (1, 2) through a second communications network; authenticating the user (22) to the application (45) by means of the mobile station (1, 2) communicating with the application (45) through the second communications network characterized in that the step of authenticating the user comprises utilizing secret information of the second communications network stored on a SIM (34) or information provided in HLR (9) and/or VLR (8) database of the second communications network; and controlling the authentication operations by means of a mobile station personal identification device (MS PAD) (35)."

XX. Each of the appellant's requests also comprises an independent claim 11 setting out an apparatus corresponding to the method of claim 1 and an independent claim (16 in the main and first auxiliary requests, 15 in the second auxiliary request) to a mobile station. For the purposes of this decision, it has not been necessary to consider these further independent claims.

Reasons for the Decision

1. *Admissibility of the appeal*

In view of the facts set out at points I to IV above, the appeal is admissible.

2. *Procedural matters*

2.1 *The cancellation of the oral proceedings*

As respondent 2 withdrew its request for oral proceedings, respondent 1 announced that it would not take part and no written substantive submissions were filed after the board had issued the summons to oral proceedings, the board had no reason to maintain the scheduled oral proceedings. The board was in a position to issue a decision according to Article 12(1) and (3) RPBA on the basis of the statement of grounds of appeal and the parties subsequent written submissions summarized above in the "facts and submissions".

2.2 *Respondent 2's auxiliary request for oral proceedings*

Respondent 2 has stated that it withdrew this request if the board were to decide as set out in its preliminary opinion in the annex to the summons to oral proceedings. Since the board does decide in this way, the condition for the withdrawal of this request is met.

2.3 *Respondent 2's request for revocation*

Respondent 2 requested the revocation of the patent in its submission dated 4 September 2007, received after expiry of the time limit for filing an appeal.

In G9/92 and G4/93, OJ EPO 1994, 875, in particular points 10 and 14 the Enlarged Board of Appeal stated that when the patent proprietor is the sole appellant the scope of its appeal as defined in its notice and statement of grounds of appeal is exceeded if the non-appealing opponent files a request for revocation of

the patent. Such a request going beyond the appellant's original appeal is not admissible.

Accordingly the request for revocation filed by respondent 2 is not admissible.

2.4 *Respondent 2's letter dated 3 September 2007*

As this letter reached the EPO after expiry of the time limit set by the board for replying to the statement of grounds of appeal, the letter forms an amendment to respondent 2's case. According to Article 13(1) RPBA (OJ EPO 2007, 536), such amendments may be admitted and considered at the board's discretion. The discretion shall be exercised in view of *inter alia* the complexity of the new subject-matter submitted, the current state of the proceedings and the need for procedural economy. The board finds that none of these considerations militates against admitting this submission and thus decides to admit respondent 2's letter into the proceedings.

3. *The context of the patent*

According to the description and figures, the patent relates to authenticating a user to an application, for instance a payment or banking service. The user accesses the application via a first communication network, which may comprise a public switched telephone network (PSTN). The user is also provided with a "mobile station" (MS) such as a GSM cellular telephone which communicates with the application via a second communications network, for example a GSM network. User authentication occurs based on secret information

stored in a SIM (subscriber identification module) in the mobile station and/or secret information stored in the HLR (home location register) and/or VLR (visitor location register) data bases stored in the GSM network.

4. *Document D1*

D1 forms the closest prior art on file and concerns the authentication of a user's identity through a variety of terminals associated with a variety of electronic services; see column 2, lines 3 to 5. To do this a user initiates service access by transmitting a request over a service access network to a service node; see column 5, lines 23 to 25. A challenge code is then transmitted via an authentication challenge network to a "personal unit", such as a cellular telephone; see column 4, lines 41 to 45, and column 5, lines 27 to 28. In view of the reference to a cellular telephone, the board regards it as implicit in D1 that communications between the service node and the personal unit involve the service node being able to connect to a database to which the personal unit is registered. The user enters a PIN into the personal unit which then calculates a unique response code using an internal algorithm and security key; see column 5, lines 30 to 34. The A3 algorithm set out in GSM 03.20 is mentioned as an example of a suitable algorithm; see column 4, lines 24 to 26. According to column 5, lines 48 to 59, the response code is transmitted via the authentication network to the service node for comparison with the expected response and, if it is acceptable, access to the service via the service access network is authorized; see column 2, lines 6 to 13. The authentication challenge network and the service access

network can be distinct and separate; see column 3, lines 44 to 46.

5. *The common general knowledge*

As already stated in the annex to the summons to oral proceedings, the board finds that recommendation GSM 03.20, set out in D2, the specifications of the SIM-ME interface, set out in D3, and the functional splitting of the GSM mobile station, set out in D4, were common general knowledge for the skilled person starting from D1 at the priority date of the present patent. Indeed D1 mentions GSM 03.20 in the "Description of Related Art"; see column 1, lines 20 to 26. The appellant has not disputed these findings.

5.1 *Document D2*

According to section 3 of D2 (see page 10), the A3 authentication algorithm according to GSM 03.20 is carried out using the same input values (the random challenge RAND and the individual subscriber authentication key Ki) both in the mobile station and in the "fixed sub-system", i.e. the network; see page 10, section 3.2, figure 3.1 and page 42, last four lines. The RAND value is generated by the network and transmitted to the mobile station. In the network the authentication key Ki is stored in the VLR and, if necessary, can be requested from the appropriate HLR; see page 11, lines 13 to 16. In the mobile station the authentication key Ki is stored in the SIM, which also contains the means for implementing the A3 algorithm. The results of the algorithm in the mobile station and the network, termed "signed responses" (SRES), are then

compared in the network to authenticate the user to the network.

5.2 *Document D3*

D3 concerns the interface between the SIM and the rest of the MS, termed the ME (Mobile Equipment). According to page 42, lines 18 to 20, when the SIM is connected to the ME the ME plays the role of master and the SIM plays the role of slave. For instance, according to page 71, lines 1 to 9, when running the A3 algorithm the MS carries out a "RUN-GSM-ALGORITHM" instruction to send the RAND value to the SIM. As the next instruction the MS must then carry out a "GET-RESPONSE" instruction (see pages 75 to 78) to read *inter alia* the SRES value, otherwise the SRES value will be lost. The board understands this to mean that the ME contains means for controlling the operation of the SIM.

5.3 *Document D4*

According to page 3, lines 8 to 9, the authentication key Ki is not readable outside the subscriber identity module and can thus be considered as "secret" information of the GSM network stored on the SIM.

6. *Novelty, Article 54(1,2) EPC 1973*

6.1 Interpreting the service access network and the authentication challenge network known from D1 as first and second communications networks, respectively, the personal unit as a mobile station and the terminal as a user interface, D1 discloses (in terms of claim 1 according to the appellant's main request) a method for

authenticating a user to an application (see column 2, lines 3 to 5), the application being available to the user through a first communications network (see figure 1; service access network 24), the method comprising: establishing a connection between the application and a user interface (see figure 1; terminal 22) through the first communications network so as to enable a user to access the application; establishing a connection between the application, which may connect to a database to which a mobile station (see figure 1; personal unit 20) is registered (see column 4, lines 41 to 45), and the mobile station through a second communications network (see figure 1; authentication challenge network 28) and authenticating the user to the application by means of the mobile station communicating with the application through the second communications network (see column 5, lines 48 to 59).

6.2 Thus it is common ground between the parties, and the board agrees, that the subject-matter of claim 1 according to the appellant's main request differs from the disclosure of D1 in the features set out in the characterizing part, namely the step of authenticating the user comprising utilizing secret information of the second communications network stored on a SIM or information provided in HLR and/or VLR database of the second communications network.

6.3 Compared to claim 1 of the main request, claim 1 of the appellant's first auxiliary request has been amended by replacing the term "or" by "and" in the expression "secret information of the second communications network stored on a SIM (34) or information provided in

HLR (9) and/or VLR (8) database of the second communications network" (emphasis added by the board). This amendment restricts the characterizing features of claim 1.

6.4 Compared to claim 1 of the appellant's main request, claim 1 of the appellant's second auxiliary request has been amended by essentially adding the expression "controlling the authentication operations by means of a mobile station personal identification device (MS PAD) (35)" at the end. As these features are not known from D1, they further characterize the subject-matter of claim 1 over the disclosure of D1.

6.5 The subject-matter of claim 1 according to the appellant's main and first and second auxiliary requests is consequently new, Article 54(1,2) EPC 1973.

6.6 It follows from the above that the objective technical problem starting from D1 proposed by the appellant, namely to provide *inter alia* a method for authenticating a user to an application, which is of low complexity and inexpensive, is already solved in D1. Hence a reformulation of the objective technical problem is required.

7. *Inventive step, Article 56 EPC 1973*

7.1 *The appellant's main request*

7.1.1 The claims of this request are the same as those of the first auxiliary request on which the appealed decision was based, the opposition division having found that

the subject-matter of claim 1 lacked inventive step, Article 56 EPC 1973, in view of D1.

7.1.2 The board regards the objective technical problem starting from D1 as being to realize the A3 algorithm of the GSM 03.20 standard in the method known from D1.

7.1.3 The board does not accept the appellant's argument that it would not have been obvious for the skilled person starting from D1 to have selected the A3 algorithm. This algorithm is explicitly mentioned in D1 (see column 4, lines 24 to 26), albeit as an example, and is thus an embodiment disclosed in D1.

7.1.4 The appellant has argued that the reference to GSM 03.20 in D1 would not have led the skilled person to use the secret code on the SIM for authenticating a user to an application. The board is not convinced by this argument, since D1 concerns the authentication of a user to an application (termed an electronic service in D1; see column 2, lines 3 to 5). The reference to GSM 03.20 in D1 would consequently have led the skilled person to use the SIM and its stored Ki value to implement the authentication process known from D1.

7.1.5 The appellant has also argued that D1 does not disclose that the secret code is secret information of the second communications network, or that the secret code is placed on the SIM card, the SIM card being provided by the operator and not the provider of the cellular phone. The board regards these details as implicit aspects of implementing the A3 algorithm, since successful authentication of the user to the network requires that the same authentication key Ki be stored

in the SIM and the HLR and/or VLR of the GSM network, it making no difference technically to system operation who provides the SIM card or stores the Ki values.

7.1.6 The board is also not convinced by the appellant's arguments that not all cellular phone systems include a SIM card and that D1 does not mention a SIM card. While these facts are not disputed, they do not change the fact that implementation of the A3 algorithm would have required the use of a SIM; see D2, page 42, lines 4 to 3 from the bottom.

7.1.7 The board concludes that the skilled person, realizing the A3 algorithm of the GSM 03.20 standard in the method known from D1, would have introduced the feature of authenticating the user by utilizing secret information of the GSM network stored on a SIM and information provided in the HLR and/or VLR database of the GSM to fill in the gaps in the disclosure of D1 without inventive step. Such a method falls within the characterizing features of claim 1, namely that authenticating the user comprises utilizing secret information of the second communications network stored on a SIM or information provided in HLR and/or VLR database of the second communications network.

7.2 *The appellant's first auxiliary request*

7.2.1 The claims of this request are the same as those of the second auxiliary request on which the appealed decision was based, the opposition division having found that the subject-matter of claim 1 lacked inventive step, Article 56 EPC 1973, in view of D1 and D2.

7.2.2 Compared to claim 1 of the main request, claim 1 of this request has been restricted by replacing the term "or" by "and" in the expression "secret information of the second communications network stored on a SIM (34) or information provided in HLR (9) and/or VLR (8) database of the second communications network" (emphasis added by the board).

7.2.3 It follows from the analysis of the main request above that the skilled person, realizing the A3 algorithm of the GSM 03.20 standard in the method known from D1, would have introduced the feature of authenticating the user by utilizing secret information of the GSM network stored on a SIM and information provided in the HLR and/or VLR database of the GSM network to fill in the gaps in the disclosure of D1, thus arriving at the subject-matter of claim 1 without inventive step.

7.3 *The appellant's second auxiliary request*

7.3.1 The claims of this request are the same as those of the third auxiliary request on which the appealed decision was based, the opposition division having found that the subject-matter of claim 1 lacked inventive step, Article 56 EPC 1973, in view of D1 and D2.

7.3.2 Compared to claim 1 of the main request, claim 1 of this request has been restricted by adding the expression "controlling the authentication operations by means of a mobile station personal identification device (MS PAD) (35)" at the end. In the light of D3, the A3 algorithm of the GSM 03.20 standard requires the use of means in the mobile station connected to the SIM for controlling the authentication procedure. Hence the

skilled person, realizing the A3 algorithm of the GSM 03.20 standard in the method known from D1, and filling in the gaps in the disclosure of D1 would have arrived at the subject-matter of claim 1 without inventive step.

7.4 *Conclusion on inventive step*

The board finds that the subject-matter of claim 1 according to the appellant's main and first and second auxiliary requests does not involve an inventive step, Article 56 EPC 1973, in view of D1 and common general knowledge (as exemplified by D2, D3 and D4).

8. *The parties' remaining requests*

Since the patent amended according to the appellant's main and first and second auxiliary requests and the invention to which it relates do not meet the requirements of the EPC, the appellant's request that the appealed decision be set aside cannot be allowed.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chairman:

C. Vodz D. H. Rees