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 3 June 2008

Case Number: T 1244/04 - 3.5.05

Application Number: 01123337.6

Publication Number: 1197827

IPC: G06F 1/00

Language of the proceedings: EN

Title of invention:
An apparatus for outputting individual authentification information

Applicant:
MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD

Opponent:
-

Headword:
Individual authentification information/MATSUSHITA

Relevant legal provisions:
EPC Art. 123(2)

Relevant legal provisions (EPC 1973):
EPC Art. 56, 83, 84

Keyword:
Inventive step - no - main request (first embodiment), first, fourth and fifth auxiliary requests (first embodiment);
Sufficiency of disclosure - no - main request (second embodiment), first auxiliary request (second embodiment);
Lack of support - yes - second auxiliary request;
Added subject-matter - yes - third auxiliary request.

Decisions cited:
-

Catchword:
-

Europäisches Patentamt | European Patent Office | Office européen des brevets

Beschwerdekammern | Boards of Appeal | Chambres de recours

Case Number: T 1244/04 **-** 3.5.05

D E C I S I O N
of the Technical Board of Appeal 3.5.05
of 3 June 2008

Appellant: MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD
1006, Oaza-Kadoma
Kadoma-shi, Osaka 571-8501 (JP)

Representative: Schwabe - Sandmair - Marx
Stuntzstrasse 16
D-81677 München (DE)

Decision under appeal: **Decision of the Examining Division of the European Patent Office posted 15 June 2004 refusing European application No. 01123337.6 pursuant to Article 97(1) EPC 1973.**

Composition of the Board:

Chairman: D. H. Rees
Members: P. Corcoran
P. Schmitz

Summary of Facts and Submissions

I. This is an appeal against the decision of the examining division to refuse the European patent application No. 01 123 337.6 published as No. 1 197 827. The decision was announced in oral proceedings held on 27 April 2004 and written reasons were dispatched on 15 June 2004.

II. The following documents have been cited during the examination and appeal proceedings:

D1: EP 0 717 339 A

D2: US 5 818 936

D3: US 5 963 908

D4: US 6 006 333

D5: B. Millar, "Vital signs of identity", IEEE Spectrum, February 1994, pp.22-30, ISSN 0018-9235.

D6: Hyun-Jung Kim, "Biometrics, Is it a Viable Proposition for Identity Authentication and Access Control ?", Computer & Security, Vol. 14, No. 3, 1995, pp.205-214, Elsevier Science Ltd., ISSN: 0167-4048.

D7: WO 1998/57247 A

D1-D3 were cited by the examining division during examination proceedings. D4 was cited in the European search report but was not subsequently referred to in proceedings before the examining division. D5-D7 are further documents introduced by the board of its own motion.

III. The decision under appeal was based on claims 1-10 filed with the letter dated 16 March 2004. The

examining division found that the subject-matter of claim 1 lacked inventive step in view of D1 combined with D3.

IV. Notice of appeal was filed and the appropriate fee paid on 13 August 2004. The notice of appeal included a precautionary request for oral proceedings. A statement setting out the grounds of appeal including a new main request and three auxiliary requests was submitted on 27 September 2004.

V. In a communication accompanying a summons to oral proceedings to be held on 3 June 2008 the board gave its preliminary opinion that none of the appellant's requests were allowable. The independent claims of the main and first auxiliary request were considered to lack inventive step in view of the available prior art combined with the skilled person's general technical knowledge in respect of biometric authentication techniques. With regard to an embodiment specifying the use of "pseudo biometric information", the board noted that, *inter alia*, it had reservations concerning compliance with the requirements of Article 83 EPC 1973.

Formal deficiencies were noted in respect of the second auxiliary request under Article 84 EPC 1973 and in respect of the third auxiliary request under Article 123(2) EPC. It was additionally noted that, even if appellant were to succeed in remedying these formal deficiencies, the board was not inclined to acknowledge an inventive step in respect of the subject-matter of these requests.

VI. With a letter of reply dated 30 April 2008, the appellant filed two further auxiliary requests and also submitted amendments to the description.

VII. At the oral proceedings the appellant requested that the decision under appeal be set aside and that a patent be granted on the basis of the claims of one of the following requests:

Claims 1-10 of the main request as filed with the statement of grounds;

Claims 1-7 of the first auxiliary request as filed with the statement of grounds;

Claims 1-9 of the second auxiliary request as filed with the statement of grounds;

Claims 1-8 of the third auxiliary request as filed with the statement of grounds;

Claims 1-4 of the fourth auxiliary request submitted on 30 April 2008;

Claims 1-11 of the fifth auxiliary request submitted on 30 April 2008.

The further documents on which the appeal is based, i.e. the text of the description and the drawings, are as follows:

Description, pages:

1-2 and 8-40 as originally filed;

3a-3b submitted on 16 March 2004.

3c-3e, 4-7 submitted on 30 April 2008.

Drawings, sheets: 1/7-7/7 as originally filed.

VIII. Claim 1 of the main request reads as follows:

"An individual authentication information output apparatus (290) connectable to a plurality of

information processing systems (310, 320) through the Internet (300), the apparatus comprising:
an input section (210) for receiving a first input from a user;
an individual authentication section (220) for outputting an individual authentication result of the user based on the first input from the user;
a specification section (230) for specifying at least an information processing system selected by the user among the plurality of information processing systems (310, 320);
a database (240) for managing individual authentication information in association with the individual authentication result provided by the individual authentication section (220) and a specification result provided by the specification section (230);
a database access section (250) for, based on the individual authentication result provided by the individual authentication section (220) and the specification result provided by the specification section (230), reading the individual authentication information associated therewith, and outputting the read individual authentication information to the selected information processing system (310, 320) through the Internet (300);
the individual authentication information is either one of biometric information and pseudo biometric information."

IX. At the end of the oral proceedings the chairman announced the board's decision.

Reasons for the Decision

1. *Main request - inventive step*

1.1 Claim 1 of the main request is substantially identical to claim 1 of the request on which the decision under appeal was based and only differs in its subject-matter in that the term "network" has been replaced by "Internet".

1.2 D1 discloses an individual authentication information output apparatus in the form of a "networking subsystem", (D1: col.5 l.17-35), which is connectable to a plurality of information processing systems through a network, (D1: col.3 l.33-38; col.4 l.10-26).

D1 further discloses the following features of claim 1:

an input section for receiving a first input from a user, (D1: col.3 l.38-40; Fig.1, ref. 24);

an individual authentication section for outputting an individual authentication result of the user based on the first input from the user, (D1: col.8 l.45 - col.9 l.2);

a specification section for specifying at least an information processing system selected by the user among the plurality of information processing systems, (D1: col.8 l.14-19);

a database for managing individual authentication information in association with the individual authentication result provided by the individual authentication section and a specification result provided by the specification section, (D1: col.9 l.16-29);

a database access section for, based on the individual authentication result provided by the individual authentication section and the specification result provided by the specification section, reading the individual authentication information associated therewith, and outputting the read individual authentication information to the selected information processing system, (D1: col.9 l.30-42).

In particular, it is noted that the "master logon" referred to in col.8 l.45 - col.9 l.2 of D1 is considered to imply functionality substantially identical to that provided by the "individual authentication section" of claim 1.

1.3 The subject-matter of claim 1 is found to differ from the disclosure of D1 in the following respects:

(i) The claim specifies that the apparatus is connectable "through the Internet" to a plurality of information processing systems whereas D1 merely refers to connectivity in the context of a network, (D1: col.4 l.10-26) and likewise to the handling of authentication requirements across multiple networks, (D1: col.5 l.36-52).

(ii) The claim specifies that the individual authentication information is either one of biometric information and pseudo biometric information whereas the disclosure of D1 with respect to authentication techniques is limited to password-based authentication.

1.4 As to the first difference identified in 1.3 above, *viz.* the specification that the apparatus is connectable to a plurality of information processing systems "through the Internet", it is noted that the term "Internet" effectively denotes a particular instance of a wide area internetwork. The application states that the network in which the invention is to be deployed "can be any type of network, for example the Internet", (cf. [0030]), but does not indicate any specific technical considerations which would arise in the context of the "Internet" as opposed to any other network.

Whereas D1 does not explicitly mention the "Internet", it nevertheless refers to the "consistent handling of authentication requirements across multiple networks", (D1: col.5 l.49-52). On this basis, the skilled person could be expected to recognise that its teaching is applicable in the context of a distributed networked environment such as the Internet.

In view of the foregoing, the board concludes that no non-obvious technical considerations are implied by the specification "through the Internet" as used in claim 1.

1.5 As to the second difference identified in 1.3 above, *viz.* the specification that "the individual authentication information is either one of biometric information and pseudo biometric information", it is noted that the wording of the claim in this respect encompasses two embodiments. According to the first embodiment the individual authentication information is "biometric information" and according to the second embodiment the

individual authentication information is "pseudo biometric information".

1.6 The disclosure of D1 concerning "individual authentication information" is limited to password-based authentication. However, the board considers that the use of biometric information for access control purposes, in particular in the context of computer systems, was generally known at the relevant priority date as was the associated technical effect, i.e. enhanced security over character-based passwords.

This has not been disputed by the appellant and is acknowledged, at least implicitly, in the application, (cf. [0008] and [0035]). Throughout the disclosure as a whole, biometric information and non-biometric information such as passwords are presented as alternative and, essentially interchangeable, forms of authentication tokens, (cf. for example: [0049], [0051], [0082], [0119] and [0121]). The application states that biometric information provides the advantage of a higher level of "reliability" than a password, (cf. [0048]), but it is nevertheless presented as having substantially the same function, i.e. to permit user authentication.

1.7 Taking due account of the aforementioned general technical knowledge of the skilled person, the use of biometric information for the purpose of authentication and access control represents an obvious alternative to the use of character-based passwords as disclosed in D1.

1.8 In view of the foregoing, the embodiment of claim 1 of the main request according to which the individual

authentication information is "biometric information", and thus claim 1 as a whole, lacks inventive step over D1 in combination with general knowledge concerning biometric authentication techniques. The main request is therefore not allowable.

2. *Main request - observations re. Article 83 EPC 1973*

2.1 The second embodiment of claim 1 of the main request according to which the individual authentication information is "pseudo biometric information" is not disclosed in the application in a manner sufficiently clear and complete for it to be carried out by a person skilled in the art.

2.2 The term "pseudo biometric information" is used in the description to denote *"information artificially produced so as to be similar to biometric information"*, (cf. [0051]). There is, however, no identifiable disclosure in the application as filed concerning the manner in which this particular category of individual authentication information is to be generated and associated with individual users in the database. Nor is, to the best of the board's knowledge, the artificial production of data which would reliably satisfy biometric authentication criteria a matter of common general knowledge in the art. The appellant has not provided any convincing evidence or arguments to the contrary in this regard.

2.3 The board therefore concludes that the application does not satisfy the requirements of Article 83 EPC 1973 in respect of the claimed invention according to the second embodiment of claim 1 of the main request.

3. *First auxiliary request*

3.1 Claim 1 of the first auxiliary request recites "an input section (210) for receiving a first input being biometric information from a user". Said claim therefore differs from the corresponding claim of the main request in that it specifies that the "first input" used for user authentication is biometric information.

3.2 As previously discussed in 1.5 above with respect to the main request, claim 1 of the first auxiliary request likewise encompasses two embodiments, *viz.* a first embodiment in which the individual authentication information is "biometric information" and a second embodiment in which the individual authentication information is "pseudo biometric information".

3.3 Replacing the password-based "master logon" of D1, (cf. D1: col.8 l.45-54) with a biometric-based authentication procedure is considered to represent a further obvious modification in the light of previously discussed general knowledge relating to biometric authentication techniques, cf. 1.6 above.

3.4 The appellant has submitted that the claimed apparatus "enables persons which for example have lost their fingers can [*sic*] access a system that only accepts fingerprint identification by using iris pattern identification input to the biometric information input section 210 which is 'transformed' by the database 240 to the required fingerprint pattern as password which can be output to the selected destination 310, 320 through the

Internet 300", (cf. statement of grounds, paragraph bridging p.3-4). This argumentation is essentially based on [0117] of the disclosure. However, the cited passage of the description relates to an embodiment according to which the individual authentication information submitted to the connection destination is "pseudo biometric information" and is *prima facie* not pertinent to first embodiment of claim 1 according to which the individual authentication information is "biometric information".

3.5 The submissions of the appellant on p.3 l.1-9 and p.4 l.7-8 of the letter dated 30 April 2008 and during oral proceedings are understood to imply that a similar effect could be obtained in the case where the "first input" and the "individual authentication information" are both biometric information, in particular different types of biometric information. The appellant effectively argues that in such a case a user who can "only sometimes" provide a specific type of biometric data required by the connection destination can nevertheless be authenticated to the connection destination by providing a different type of biometric information as the "first input".

In this regard it is noted that there is no identifiable disclosure in the application as filed of any particular technical effect in respect of using biometric information for authentication at the user terminal and at the destination information processing system as required by the first embodiment of claim 1.

The board further takes the view that, insofar as said first embodiment might arguably be capable of providing the alleged effect, in particular where different types

of biometric information are chosen for the "first input" and the "individual authentication information", such an effect would not imply the presence of an inventive step. In the given circumstances it would be merely an additional "bonus effect" following from an obvious design choice, i.e. the use of biometric data rather than passwords for user authentication at two separate access control points of a distributed data processing system.

3.6 In view of the foregoing, the board does not accept the merits of the applicant's submissions in respect of the first embodiment of claim 1 of the first auxiliary request according to which the individual authentication information is "biometric information". Said embodiment, and thus claim 1 as a whole, lacks inventive step over D1 in combination with general knowledge concerning biometric authentication techniques. The first auxiliary request is therefore not allowable.

3.7 The board additionally notes that the application does not comply with the requirements of Article 83 EPC 1973 in respect of the second embodiment of claim 1 of the request according to which the individual authentication information is "pseudo biometric information" for substantially the same reasons given in 2. above in relation to the corresponding embodiment of claim 1 of the main request.

4. *Second auxiliary request*

4.1 Claim 1 of the second auxiliary request is based on claim 1 of the main request combined with the features of dependent claim 2 of the main request, *viz.*:

> "the individual authentication information output apparatus (290) is connectable to a plurality of terminals through the network (300), wherein the plurality of terminals include:
>
> a first terminal having a first input section for receiving the first input of a first type input from the user; and
>
> a second terminal having a second input section for receiving a second type input, which is different from the first type input, from a user, the first type input and the second type input being provided to the input section of the individual authentication information output apparatus (290) through the network (300)".

Additionally, the term "Internet" has been replaced by "network" throughout the claim.

4.2 According to the appellant the independent claim of this request is based on the preferred embodiment of "Example 2" of the description, (cf. statement of grounds, p.5 l.4). The disclosure relating to "Example 2" states that the "individual authentication section" is capable of handling both iris and fingerprint patterns, (cf. [0081]). In its most general form this embodiment envisages an "individual authentication section" which can process N different types of input "patterns" which may be either biometric or non-biometric, e.g. passwords, (cf. [0082]).

4.3 The claim initially specifies "an input section (210)" comprised within the apparatus itself and subsequently "a first input section" associated with a first terminal and "a second input section" associated with a second terminal. This is not consistent with the embodiment according to "Example 2" because the apparatus (400) does not have an "input section (210)". According to this embodiment, the only input sections, 430 and 435, are those located in the terminals, 420 and 425, (cf. Fig. 2).

The wording of the claim likewise fails to specify that the "individual authentication section" is capable of processing a plurality of different types of "input patterns" which is considered to be an essential feature of this embodiment, (cf. [0082]). The claim recites a plurality of terminals which can receive inputs of different types ("first type input" and "second type input") and then specifies that these inputs are provided to the "input section" of the apparatus. The embodiment on which the claim is allegedly based would require that the inputs are provided to the "individual authentication section" of the apparatus.

4.4 In view of the foregoing, claim 1 of the second auxiliary request does not comply with the requirements of Article 84 EPC 1973 because it defines the matter for which protection is sought in a manner which is not supported by the description.

4.5 The request is therefore not allowable. In view of the aforementioned deficiency it is not necessary to consider the additional objections raised by the board in its

communication accompanying the summons to oral proceedings.

5. *Third auxiliary request*

5.1 Claim 1 of the third auxiliary request is based on claim 1 of the main request with the following additional features derived from dependent claims 4 and 5 of the main request:

"the individual authentication information output apparatus (290) is connectable to a plurality of terminals through the network (300), wherein the plurality of terminals include:

a first terminal having a first input section for receiving the first input of a first type from the user, the first input being provided to the input section of the individual authentication information output apparatus (290) through the network (300), wherein:

the first input of the first type is individual authentication information of a first type and the read individual authentication information is individual authentication information of a second type,

and the first type and second type individual authentication information are of different types, and

the first type individual authentication information is either one of a password, biometric information and pseudo biometric information".

As in the case of the preceding request, the term "network" is used instead of "Internet" throughout the claim.

5.2 The part of the claim based on claim 1 of the main request specifies that *"the individual authentication information is either one of biometric information and pseudo biometric information"*. This is understood to refer to the authentication data read from the database and used to access the destination connection. The additional features of the claim introduce a further category of "individual authentication information", which is defined as "individual authentication information of the first type" and which is understood to denote the authentication information input when a user is prompted following an attempt to access a destination connection. The claim specifies that this information input by the user is either one of "a password, biometric information and pseudo biometric information".

5.3 The use of "pseudo biometric information" as a user input is, however, not disclosed in the application as filed according to which the user inputs are always either biometric information or non-biometric information (e.g. passwords) but never "pseudo biometric information". "Pseudo biometric information" is only disclosed as one of the possible forms of the authentication information retrieved from the database. Consequently, this amendment infringes Article 123(2) EPC.

5.4 The request is therefore not allowable. In view of the aforementioned deficiency it is not necessary to consider the additional objections raised by the board in its

communication accompanying the summons to oral proceedings.

6. *Fourth auxiliary request*

6.1 Claim 1 of the fourth auxiliary request is based on claim 1 the first auxiliary request with the following additional features derived from claims 4 and 5 of said request:

"wherein biometric information represents a type of the types of fingerprint, face, retina, iris, handprint, voice and handwriting;

wherein the individual authentication information is biometric information;

wherein the biometric information inputted by the user is of a first type and the individual authentication information is of a second type;

wherein the first type is different to the second type".

As in the case of the preceding request, the term "network" is used instead of "Internet" throughout the claim.

6.2 The subject-matter of the claim is distinguished from that of claim 1 of the first auxiliary request in the following respects:

(i) The "individual authentication information" retrieved from the database is specified as biometric information and the option of pseudo biometric information has been deleted.

(ii) The claim defines biometric information as representing one of the following "types": fingerprint, face, retina, iris, handprint, voice and handwriting.

(iii) The claim further specifies that the "first input" used for user authentication and the "individual authentication information" retrieved from the database are different types of biometric information.

6.3 The first difference identified in 6.2 above implies that claim 1 of the fourth auxiliary request is limited to an embodiment in which both the "first input" used for user authentication and the "individual authentication information" retrieved from the database are both biometric information. As noted previously in 1.6, the use of biometric information for the purpose of user authentication represents an obvious alternative to the use of character-based passwords.

6.4 The second difference identified in 6.2 above is a definition of the term "biometric information" by way of an enumeration of various categories of biometric information. This merely acts to define the scope of the term "biometric information" in terms of a subset of known types of biometric information and, as such, does not imply any non-obvious technical considerations.

6.5 The third difference identified in 6.2 above effectively specifies that a first type of biometric information is required for authentication at the user terminal, and

that a second, different type of biometric information is required for authentication at the connection destination. Specifying different types of biometric information for user authentication at different access control points of a distributed data processing system is considered to be a matter of design choice not requiring the exercise of inventive skill.

6.6 The appellant has argued that by receiving a first type of biometric information, (i.e. the "first input"), and returning a second type of biometric information, (i.e. the "individual authentication information" which is retrieved from the database and submitted to gain access to the connection destination), the claimed apparatus provides access to a network service that requires transmission of one specific type of biometric data which, for example, a handicapped person can only sometimes or never provide, (cf. letter dated 30 April 2008, p.3 l.1-9). The board does not accept the merits of these arguments for substantially the same reasons as given in 3.4 and 3.5 above.

In particular, claim 1 of the present request is understood to be based on [0099] - [0122] of the description relating to "Example 3" as illustrated in Fig. 6. According to the description, each of the first and second type of individual authentication information can be "any type of individual authentication information usable for individual authentication", (cf. [0119], emphasis added). No specific technical effect can be derived from the relevant passages of the description in respect of selecting a first type of biometric information for authentication at the user terminal and a second, different type of biometric information for

authentication at the connection destination information processing system.

6.7 In view of the foregoing, claim 1 of the fourth auxiliary request lacks inventive step over D1 combined with general knowledge for substantially the same reasons advanced in respect of the corresponding claim of the first auxiliary request in 4. above. The additional features of the present claim 1 defining the use of different types of biometric information selected from a subset of known types of biometric information relate to matters of design choice not requiring the exercise of inventive skill. The fourth auxiliary request is therefore not allowable.

7. *Fifth auxiliary request*

7.1 Claim 1 of the fifth auxiliary request is based on original claims 9 and 11 and differs in substance from claim 1 of the preceding request in that it recites that the claimed apparatus is "connectable to a plurality of terminals" and that:

> "the plurality of terminals (420, 425) include a first terminal (420) having a first input section (430) for receiving first type individual authentication information from a user, the first type individual authentication information being provided to the individual authentication information output apparatus (600) through the network (300)",

and in that the "individual authentication section" is omitted.

7.2 The specifications that the claimed apparatus is "connectable to a plurality of terminals" and that the "input section ... for receiving a first input" forms part of a first terminal of the plurality of terminals define an arrangement according to which the database for managing the individual authentication information is accessible from a plurality of user terminals via a network.

7.3 D2 which relates to a distributed authentication service available throughout an entire network, (cf. D2: col.4 l.15-20), is thus considered to represent closer prior art to the subject-matter of claim 1 of the present request.

7.4 D2 discloses an individual authentication information output apparatus in the form of an "exchange controller" for automating a distributed authentication service, (cf. D2: abstract; col.3 l.24-30), which is connectable to a plurality of terminals ("workstations") and a plurality of information processing systems through a network, (cf. D2: col.4 l.12-20).

It is considered implicit in the disclosure of D2 that the plurality of terminals include a first terminal having a first input section for receiving first type individual authentication information from a user, ("user secret", cf. D2: col.5 l.14-22).

7.5 The apparatus of D2 further comprises:

a database ("authentication database") for managing second type individual authentication information in association with the first type individual authentication information, (cf. D2: col.3 l.27-31; col.6 l.12-21); and

a database access section for, based on the first type individual authentication information, reading the second type individual authentication information associated therewith, and outputting the read second type individual authentication information to a selected information processing system among the plurality of information processing systems through the network, (cf. D2: col.6 l.60 - col.7 l.9).

7.6 The subject-matter of claim 1 is thus distinguished from the disclosure of D2 in the following respects:

(i) The claim specifies that the first type individual authentication information is a first type of biometric information whereas D2 merely discloses user authentication at the terminal ("workstation") based on the input of a "user secret" which may be, for example, a password, (cf. D2: col.5 l.14-22).

(ii) The claim further specifies that the second type individual authentication information retrieved from the database is a second type of biometric information whereas D2 merely discloses that user authentication at the destination information

processing systems is by means of "application secrets", which can be passwords, (cf. D2: col.2 l.25-27; col.3 l.25-53).

7.7 With regard to the differences identified in 7.6 above, the board takes the view that, starting from D2, the selection of different types of biometric authentication information to be used in respect of the authentication procedure at the terminal and the authentication procedure at the destination information processing systems represents a matter of design choice not requiring the exercise of inventive skill when due account is taken of the relevant general knowledge in respect of biometric authentication techniques as discussed under 1.6 above.

Referring to 6.6 above, no specific technical effect in respect of selecting a first type of biometric information for authentication at a user terminal, and a second, different type of biometric information for authentication at a destination information processing system can be derived from the supporting passages of the description.

7.8 The appellant has submitted arguments concerning the alleged advantages provided by the claimed apparatus of the present request which are substantially similar to those referred to under 6.6 above in respect of the preceding request, (cf. letter dated 30 April 2008, p.4 l.1-9). The board does not, however, accept the merits of the arguments submitted by the appellant in respect of the present request for substantially the same reasons as given in 6.6 above, (see also 3.4 and 3.5).

7.9 During oral proceedings, the appellant raised the question as whether it would be obvious to use biometric information for the user input in a system such as that disclosed in D2, given that said document refers to deriving an encryption key from a password entered at a user terminal, (cf. D2: col.2 l.5-17). The appellant's submissions on this point appear to be based on the premise that the teaching of D2 requires user input in the form of a cryptographic key and that it would not represent an obvious modification of this teaching to replace a cryptographic key by a biometric input.

The board is, however, unable to follow the appellant's arguments in this regard. In particular, it is noted that the cited passage of D2 on col.2 l.5-17 refers to background prior art rather than the distributed authentication service which forms the subject of D2. From col.5 l.14-22 of D2 it is evident that the distributed authentication service of D2 requires a user to input an authentication token ("user secret") which may be, for example, a password. The use of biometric information represents an obvious alternative to the use of character-based passwords as discussed in 1.6 above. The board cannot identify any convincing reason which would exclude the use of biometric information as a "user secret" in the context of the authentication procedure at the user terminal as disclosed in col.5 l.14-22 of D2.

7.10 In view of the foregoing, the board finds that claim 1 of the fifth auxiliary request lacks inventive step over D2 in combination with general knowledge in respect of

biometric authentication techniques. The request is therefore not allowable.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chairman:

K. Götz D. H. Rees