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 28 June 2022

Case Number:	T 0602/19 - 3.4.03
Application Number:	11725701.4
Publication Number:	2580723
IPC:	G06Q20/00, G06F21/00
Language of the proceedings:	EN

Title of invention:

A METHOD AND SYSTEM FOR PROVIDING UNIVERSAL ACCESS TO A SERVICE AMONGST A PLURALITY OF SERVICES

Applicant:

Pay & Save N.V.
Maris, Johan

Headword:

Relevant legal provisions:

EPC Art. 56, 123(2)
RPBA Art. 12(4)

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

Keyword:

Inventive step - (no)
Late-filed request - submitted with the statement of grounds of appeal - admitted (no) - request could have been filed in first instance proceedings (yes)

Decisions cited:

T 1362/19

Catchword:

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
Fax +49 (0)89 2399-4465

Case Number: T 0602/19 - 3.4.03

DECISION
of Technical Board of Appeal 3.4.03
of 28 June 2022

Appellant:
(Applicant 1)

Pay & Save N.V.
Ambachtenstraat 11A
3210 Lubbeek (BE)

Appellant:
(Applicant 2)

Maris, Johan
Ambachtenstraat 11A
3210 Lubbeek (BE)

Representative:

BiiP cvba
Engels Plein 3 bus 102
3000 Leuven (BE)

Decision under appeal:

Decision of the Examining Division of the European Patent Office posted on 1 October 2018 refusing European patent application No. 11725701.4 pursuant to Article 97(2) EPC.

Composition of the Board:

Chairman M. Stenger
Members: A. Böhm-Pélissier
E. Mille

Summary of Facts and Submissions

I. The appeal is against the decision of the Examining Division to refuse the Main Request of patent application No. 11 725 701. The refusal was based on the ground of lack of inventive step (Article 56 EPC) over D1 in combination with the common general knowledge. The decision was a decision according to the state of the file and referred to the summons dated 1 February 2018.

II. Reference is made to the following **documents**:

D1 = US 2006/0191995 A1
D4 = WO 01/75744 A1
D5 = JP 2008/217626 A

III. Oral proceedings took place on 28 June 2022. With letter of 8 June 2022, the Appellant informed the Board that he would not attend the oral proceedings.

IV. The Appellant (applicant) **requests** that a patent be granted based on a Main Request or alternatively on one of Auxiliary Requests 1 to 7, all filed with the statement of grounds of appeal on 11 February 2019.

V. **Claim 1** according to the **Main Request** reads (labelling (A), (B), ... added by the Board):
(A) A method for providing universal access to a service amongst a plurality of services comprising:
(B) storing a plurality of service accounts, each corresponding to a customer and a service said customer is subscribed to,

(C) receiving a request from a customer for using a service,
(D) determining a service account corresponding to said customer and said service,
(E) consulting confidential service account content corresponding to said service account, characterized in that
(F) said service account is determined upon identifying such customer and the requested service or its service provider,
(G) wherein identifying such customer comprises hashing any available identification instrument of a number of identification instruments linked to said customer's identification code,
(H) and in that said consulting comprising real-time communicating with said service provider, said service provider providing real-time access to said confidential service account content.

Claim 1 of the **Auxiliary Request 1:**
Feature (H) in the Main Request is replaced by Feature (H1) (highlighting [additions, ~~deletions~~] of amendments with respect to the Main Request added by the Board):
(H1) and in that said consulting comprising querying said confidential service account content via real-time communicating with said service provider, said service provider providing real-time access to ~~said~~ its confidential service account content.

Claim 1 of the **Auxiliary Request 2:**
Feature (F) in the Auxiliary Request 1 is replaced by Feature (F2) (highlighting with respect to the Main Request):
(F2) determining said service account is ~~determined upon identifying such~~ based on the identity of the customer and the ~~requested service or its service~~

~~provider~~ origin of said request,

Claim 1 of the **Auxiliary Request 3:**
Features (F) and (H) in the Main Request are replaced by Features (F3) and (H3) (highlighting with respect to the Main Request):
(F3) said service account is determined upon identifying such customer and the ~~requested service or its service provider~~ origin of the request
(H3) and in that said consulting ~~comprising~~ of confidential service account content consists of querying said confidential service account content via real-time communicating with said service provider, said service provider providing real-time access to ~~said~~ its confidential service account content.

Claim 1 of **Auxiliary Request 4:**
Features (B) and (H) in the Main Request are replaced by Features (B4) and (H4) (highlighting with respect to the Main Request):
(B4) storing a plurality of service accounts in a service account database, each service account corresponding to a customer and a service said customer is subscribed to,
(H4) and in that said confidential service account content is not stored in said service account database and that said consulting comprising querying said confidential service account content via real-time communicating with said service provider, said service provider providing real-time access to ~~said~~
its confidential service account content.

Claim 1 of **Auxiliary Request 5:**
Feature (F) in the Auxiliary Request 4 is replaced by Feature (F5) (highlighting with respect to the Main Request):

(F5) in that the determination means are adapted for determining said service account ~~is determined upon identifying such~~ based on the identity of the customer and the ~~requested service or its service provider~~ origin of the request,

Claim 1 of **Auxiliary Request 6:**
Feature (H4) in the Auxiliary Request 4 is replaced by Feature (H6) (highlighting with respect to the Main Request):
(H6) in that only information needed for identification of the customer and the requested service or its service provider is stored in the service account database and that said confidential service account content is not stored in said service account database, and that said consulting comprising querying said confidential service account content via real-time communicating with said service provider, said service provider providing real-time access to ~~said~~ its confidential service account content.

Claim 1 of **Auxiliary Request 7:**
Feature (F) of Auxiliary Request 6 is replaced by Feature (F2).

VI. The Appellant argued essentially as follows in his written submissions:

(a) D1 nowhere disclosed or taught to determine a service account upon identifying the customer and the requested service or service provider wherein said identifying is done by hashing any available identification instrument.

(b) D1 furthermore did neither disclose nor teach real-time communication.

Reasons for the Decision

1. The appeal is admissible.

2. The invention as claimed

2.1 Customers collect loyalty cards, bank cards, credit cards, badges, and other identification instruments associated with all kinds of services they are subscribed to. It is difficult to maintain such large number of cards and either to continuously carry them all in a handbag or a wallet, either to make sure having the correct valid card available upon using a service or visiting a store or a bank. This may be overcome by collecting account information on a central server. This however implies that the service provider has to share confidential service account content with the universal access system. Another disadvantage is that service account content has to be duplicated and updated in the universal access system database from the service provider's database, which means a waste of memory space. (description, page 1, line 11, to page 2, line 8, of the present patent application).

2.2 This should be overcome by the present invention by saving account data on a server, which is secured by encryption using "hashing" and which can be consulted via real-time communication.

3. Main Request - Inventive Step

3.1 Closest prior art

D1 discloses a method similar to the present invention but does not explicitly disclose "real-time communication" and "hashing" as follows.

3.2 D1

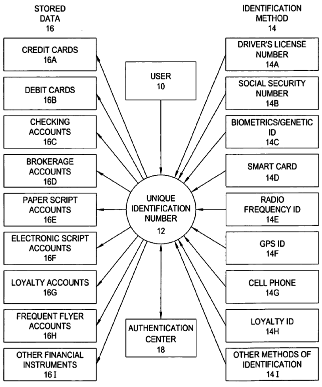
STORED DATA 16
CREDIT CARDS 16A
DEBIT CARDS 16B
CHECKING ACCOUNTS 16C
BROKERAGE ACCOUNTS 16D
PAPER SCRIPT ACCOUNTS 16E
ELECTRONIC SCRIPT ACCOUNTS 16F
LOYALTY ACCOUNTS 16G
FREQUENT FLYER ACCOUNTS 16H
OTHER FINANCIAL INSTRUMENTS 16I
USER 10
UNIQUE IDENTIFICATION NUMBER 12
AUTHENTICATION CENTER 18
IDENTIFICATION METHOD 14
DRIVER'S LICENSE NUMBER 14A
SOCIAL SECURITY NUMBER 14B
BIOMETRICS/GENETIC ID 14C
SMART CARD 14D
RADIO FREQUENCY ID 14E
GPS ID 14F
CELL PHONE 14G
LOYALTY ID 14H
OTHER METHODS OF IDENTIFICATION 14I

FIG. 1

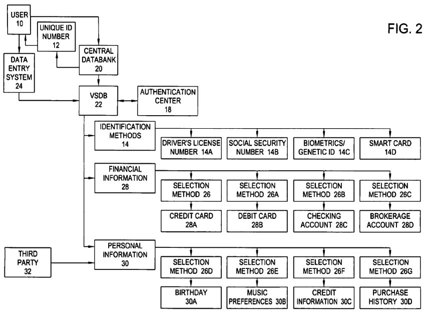

FIG. 2

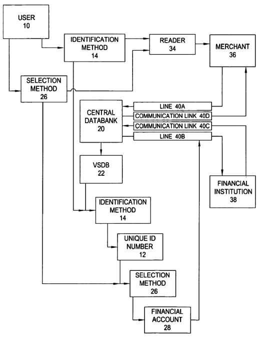

FIG. 3

D1

3.2.1 Features (A) to (D): D1 discloses that client data and account data ("STORED DATA" in Fig. 1 saved in "CENTRAL DATABANK 20" in Fig. 2) is saved on a server (Fig. 2, "CENTRAL DATABANK 20", separate database "VSDB 22" comprising "FINANCIAL INFORMATION 28" and "PERSONAL INFORMATION 30"). In D1 the user ("USER 10") can access multiple services by means of a "UNIQUE ID NUMBER 12".

3.2.2 Features (E) and (H): There is no indication in D1 that the communication in general is not a real-time communication, in particular for the embodiment shown in Fig. 3 and disclosed in paragraphs [0041] to [0047]. In all embodiments the information is sent directly to the requester. D1 ([0056], last but one sentence ff) e.g., discloses that the information is sent directly to the third party. This is understood in the sense that per default data is sent directly, i.e. by real-time transmission.

3.2.3 In the present application "confidential service account content" is part of the data saved in the service provider's database (SPD1 to SPD3). In analogy to this, the "FINANCIAL INSTITUTION 38" in D1 (cf. Fig. 3) also comprises "confidential service account content". Furthermore, paragraph [0047] (financial account information 28) and Fig. 3 in combination with paragraph [0022] (access to the financial account data via financial institution 38) of D1 disclose that the "confidential service account content" is saved on a separate database (38) with respect to central database 20 and that at no time "confidential service account content" from the financial institution 38 is forwarded to an external party, i.e. "MERCHANT 36" (Fig. 3). Central database 20 must query the "confidential service account content", i.e., account data necessary for the financial transaction, in financial institution 38 to accomplish the financial transaction.

3.2.4 In another approach the "PERSONAL INFORMATION 30" (cf. Fig. 2) is considered to correspond to the "confidential service account content". Personal data 30 is saved elsewhere (in VSDB 22) than in the central database (20). D1 discloses in paragraphs [0056] and [0057] querying for the confidential personal data ("Is user 2 twenty-one years of age or older?").

3.2.5 Furthermore, Paragraphs [0045], [0046], [0052] and [0056] to [0057] disclose that the third party 32/36 needs to be registered and must be identified and authenticated prior to accessing and querying confidential data 30/38. Therefore, the skilled person understands that - for security reasons - identification and authentication as well as the further processing and querying takes place with real-time communication.

3.2.6 Consequently, the aforementioned passages provide no hint that any other type of communication than real-time communication takes place for identifications, consulting, querying and for providing access to (confidential) service account content.

3.2.7 Feature (G): For the identification method 14 the communication is encrypted ([0047]).

3.2.8 D1 therefore discloses that a service account is determined upon identifying the customer and the requested service or service provider, wherein said identifying is done by encrypting any available identification instrument of a number of identification instruments (14) linked to said customer’s identification code, and that upon consulting the confidential service account content (38/30), the service provider provides direct (in "real-time") access to the confidential service account content.

3.3 Disclosure of D1 in the wording of claim 1

3.3.1 D1 therefore discloses (labeling (A), (B), ..., references with respect to D1 [cf. Figs. 1 to 3] and highlighting [addition, ~~deletion~~] of differences with respect to present claim 1 added by the Board):

(A) A method for providing universal access to a service amongst a plurality of services comprising:

(B) storing a plurality of service accounts ("STORED DATA 16"), each corresponding to a customer and a service ("FINANCIAL INFORMATION 28" in Fig. 2) said customer is subscribed to (in a service account database "CENTRAL DATABANK 20" in Fig. 2),

(C) receiving a request from a customer ("USER 10" in Figs. 2 and 3) for using a service,

(D) determining a service account corresponding to said customer and said service ([0047]: Central Databank 20 determines "USER 10"'s Unique Identification Number, Central Databank determines which of the available accounts "USER 10" has selected),

(E) consulting (by "MERCHANT 36" or "THIRD PARTY 32) confidential service account content corresponding to said service account (from "LINE 40B" to "FINANCIAL INSTITUTION 38" in Fig. 3, querying cf. [0047]; querying confidential personal information 30: cf. [0056] and Fig. 2; or alternatively from "THIRD PARTY 32" to VSDB database 22 containing detailed account data 28 and "PERSONAL INFORMATION 30"),
(F) ~~characterized in~~ wherein said service account is determined upon identifying such customer ("IDENTIFICATION METHOD 14" in Fig. 1, [0039]-[0041]) and the requested service or its service provider,
(G) wherein identifying such customer comprises ~~hashing~~ encrypting ([0047] and [0049]) any available identification instrument of a number of identification instruments (14) linked to said customer's identification code,
(H) and in that said consulting ([0047], [0056], [0057]) comprising real-time communicating with said service provider, said service provider providing real-time access to said confidential service account content (cf. sections 3.2.2 to 3.2.6 above).

3.4 Difference

3.4.1 D1 therefore does not disclose that the encryption defined in feature (G) consists in hashing the identification instrument.

3.4.2 The Appellant argued that in the invention only one identification code in combination with the requested service or its service provider was required for determination of the service account, whereas in D1 an "IDENTIFICATION METHOD 14" was applied.

3.4.3 The Board however concludes that Features (A) to (D) do not exclude that the unique identification number may be accessed via an "IDENTIFICATION METHOD 14" (cf. Figs. 1, 2) using a driver license number or social security number, which is again one single identification item ([0025], sixth sentence ff.).

3.4.4 The Appellant argued that in [0022] the system of D1 communicated with a financial institution, but did not consult the confidential service account content of that financial institution.

3.4.5 The Board however concludes that financial account data can be considered as "confidential service account content corresponding to said service account".

3.4.6 In T1362/19 (catchword) the Board held that if an abstract feature is not defined in more concrete terms either in the relevant claim or in the description it has to be understood in a broad sense. This is important when assessing the implicit disclosure of a document of the state of the art.

3.4.7 The claim and the application do not provide any technical details in relation to real-time communication. In the absence of any specification how the "real-time" communication takes place, this term has to be construed in a broad manner and thus can be read on the disclosure of D1, i.e., the encrypted direct (and not in any way delayed) communication disclosed in paragraphs [0047] and [0056] requiring authentication. Consequently, Feature (H) is disclosed by D1.

3.5 Effect / Problem

The problem solved by the differentiating feature ("hashing") relates to choosing a suitable encryption method.

3.6 Obviousness

3.6.1 In the context of secure data transfer, hashing is a common option for encrypting confidential data. E.g., D4 teaches hashing in the context of a secured identification procedure (claim 29, Feature B.); D5 also teaches hashing for authentication ([0005]: "*In addition ... it is possible to use a value other than the actual user ID (for example, a hash value or a value changed for each service providing server) for the user ID to be authenticated ...*").

3.6.2 It is therefore obvious to use hashing as the encryption method mentioned in paragraphs [0047] and [0049] in D1. Consequently, the subject-matter of claim 1 of the Main Request is obvious over the disclosure of D1 in combination with the common general knowledge and is not inventive within the meaning of Article 56 EPC.

4. Auxiliary Requests 1 to 7 - Article 12(4) RPBA 2007

4.1 Auxiliary Requests 1 to 7 have been introduced with the statement of grounds of appeal. The Board does not admit these requests under Article 12(4) RPBA 2007 because the requests should have been filed already before the Examining Division, e.g., in response to the summons to oral proceedings or during oral proceedings. The Applicant however had decided not to attend the oral proceedings, where such requests could have been discussed with the Examining Division. The Board could then have dealt with the reasoning of the Examining

Division and would not have had to examine Auxiliary Requests 1 to 7 for the first time.

4.2 The Board notes that the subject-matter of claim 1 of Auxiliary Request 1 to 7 is further not allowable under Article 123(2) and 56 EPC as discussed in the communication preparing the oral proceedings.

5. Conclusions

Since the subject-matter of claim 1 according to the Main Request does not involve an inventive step and Auxiliary Requests 1 to 7 are not admitted into the proceedings pursuant to Article 12(4) RPBA 2007, the appeal must fail.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chairman:

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

B. Atienza Vivancos M. Stenger

Decision electronically authenticated