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 December 2022

Case Number:	T 3267/19 - 3.5.06
Application Number:	13702216.6
Publication Number:	2951749
IPC:	G06F21/34, G06Q20/40
Language of the proceedings:	EN

Title of invention:
REGISTERING A MOBILE USER

Applicant:
Barclays Execution Services Limited

Headword:
Registering a mobile user/BARCLAYS

Relevant legal provisions:
EPC Art. 56
RPBA 2020 Art. 13(2)

Keyword:
"Fourth" to "seventh" auxiliary requests - filed in response to the summons to oral proceedings - admitted (yes) - inventive step (no)
"Eighth" auxiliary request - filed during oral proceedings - admitted (no)

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

Decisions cited:
T 1294/16

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 3267/19 - 3.5.06

DECISION
of Technical Board of Appeal 3.5.06
of 15 December 2022

Appellant:
(Applicant)

Barclays Execution Services Limited
1 Churchill Place
London E14 5HP (GB)

Representative:

Carpmaels & Ransford LLP
One Southampton Row
London WC1B 5HA (GB)

Decision under appeal:

Decision of the Examining Division of the European Patent Office posted on 23 July 2019 refusing European patent application No. 13702216.6 pursuant to Article 97(2) EPC.

Composition of the Board:

Chairman	M. Müller
Members:	G. Zucka
	W. Sekretaruk

Summary of Facts and Submissions

I. The appeal is against the decision of the examining division to refuse European patent application no. 13702216 for lack of inventive step as the implementation of a non-technical business process on commonly known networked mobile devices. A number of documents were referred to. For the present decision, only the following ones are of interest:

D2: Wikipedia, "Mobile banking", 2013, retrieved from the Internet at https://en.wikipedia.org/w/index.php?title=Mobile_banking&oldid=534279834, retrieved on 8 January 2018 (XP055438875),
D6: Wikipedia, "Authentication", 2013, retrieved from the Internet at https://en.wikipedia.org/w/index.php?title=Authentication&oldid=534502493, retrieved 8 January 2018 (XP055538892),
D8: Missnatalia, "Verification Processes for Customers at Skrill", 2012, retrieved from the Internet at https://www.pokerstrategy.com/forum/thread.php?threadid=172379, retrieved 8 January 2018 (XP055438757), and
D13: US 2011/151890 A1.

II. An appeal was filed on 30 September 2019, the appeal fee paid on the same day. A statement of grounds of appeal was received on 25 November 2019. The appellant requested that the decision be set aside and a patent be granted on the basis of claims according to a main request or to one of three auxiliary requests.

III. With its summons to oral proceedings, the board informed the appellant of its preliminary opinion that the claims of all requests lacked clarity, Article 84

EPC. It left open the question whether or to what extent the claimed subject matter made a technical contribution but stated that it appeared to lack an inventive step over common general knowledge alone or, alternatively, over document D13 in combination with D8 and common general knowledge, Article 56 EPC.

IV. In response to the summons, the appellant filed amended sets of claims labelled as, respectively, "fourth" to "seventh" auxiliary requests. During the oral proceedings, and in response to the board's indication that it would admit the new requests, the appellant withdrew the higher-ranking requests. It also filed a further set of claims labelled "eighth" auxiliary request.

V. Claim 1 of the request labelled the "fourth" auxiliary request reads as follows:

"A method of registering a user of a mobile device, wherein the user sets an access password, pass phrase, pass code or pass number when a mobile application of the mobile device is first run before registration takes place, the method of registering comprising the steps of:

obtaining, by the mobile application from the user, data identifying the user and account data;

retrieving, by the mobile application, data uniquely identifying a mobile device, wherein the data uniquely identifying the mobile device is any one or more selected from the group consisting of: MAC address, WiFi identifier, international mobile subscriber identity, IMSI, unique identifier ID, UDID, near field communication, NFC Identifier, MSISDN, and IMEI;

authenticating, by the mobile application, the user with the mobile device, using the password, pass phrase, pass code or pass number as a challenge, wherein the correct access password, pass phrase, pass code or pass number is required from the user before the user is registered; and

transmitting, by the mobile application to a server over a network and the internet, the data identifying the user, the account data, and the data uniquely identifying the mobile device;

validating, by the server, the user with the account using the data identifying the user and the account data and the data uniquely identifying the mobile device, and

if the user is validated, then registering the user and adding the user to a registration database,

if the user is not validated, then not registering the user or marking the user as unvalidated in the registration database."

VI. Claim 1 of the auxiliary request labelled the "fifth" differs from the "fourth" in the following additional feature at its end:

"... wherein, if the method of registering is only partially complete then presenting to the user an access password, pass phrase, pass code or pass number challenge to verify the user before registration progresses or completes."

VII. Claim 1 of the auxiliary request labelled the "sixth" differs from the "fifth" in that the validating step is further defined by the additional clause:

"... wherein validating the user comprises the steps of: sending a payment with a reference to the account; and receiving from the user the reference; ..."

VIII. Claim 1 of the auxiliary request labelled the "seventh" differs from the "sixth" in that it also contains the text that was added to the "fifth".

IX. Claim 1 of the auxiliary request labelled the "eighth" differs from the "seventh" in that the clause of "adding the user to a registration database" is qualified by the clause

"... such that the registered user can engage in peer-to-peer payments and obtain other services using the mobile application and operation of the mobile application on another mobile device for the account is prevented; ..."

X. Oral proceedings took place on 15 December 2022, at the end of which the chairman announced the decision of the board.

Reasons for the Decision

Admittance issues

1. All present requests being filed after the board's preliminary opinion, their admittance is governed by Article 13(2) RPBA 2020. The claims according to the "fifth" to the "seventh" auxiliary requests were amended as a response to the board's objections under Article 84 EPC, and successfully overcome at least some of them. Since these requests did not introduce any new problems and could therefore be discussed during the oral proceedings without any detriment to procedural economy, the board decided to admit them (cf. T 1294/16, points 18.3 and 18.4 of the reasons). The

"eighth" auxiliary request was filed during the oral proceedings, after an extensive discussion of the previous requests and in an attempt to overcome the board's inventive step objection. Since this request was filed at a very late stage of the proceedings, did not appear to overcome the inventive step objection and raised a new clarity concern (see below), the board decided not to admit it.

The invention

2. The application is concerned with providing a secure and convenient way for users to access their financial accounts via their mobile device. As a solution, implemented in an application running on the mobile device, a novel "triangle of trust" is said to be provided between the user, the mobile device and the bank account (see, in particular page 7, paragraph 1). This triangle is "formed" by confirming that a user is associated with their own bank account and binding the user to the mobile device, which is said to ensure that the account can only be accessed by the specific mobile phone (*loc. cit.*, page 10, paragraph 4, and page 11, paragraph 2). In the process, the user sets a pass code or such like when the application is run first, a unique identity of the mobile device is retrieved, and a pass code challenge is provided to the user (see page 3, paragraph 1; page 8, paragraph 3; and page 8, last paragraph, to page 9, paragraph 1). The financial account indicated by the user is validated by sending a small payment to the account along with a "payment reference code" and requiring the user to input that code in the mobile application as a proof that they actually have access to the account (see page 10, last paragraph). Only when both validations are successful, is the user registered for accessing their account (see

e.g. page 10, paragraph 3, and the paragraph bridging pages 10 and 11).

Technical contribution

3. The examining division has stated in general terms that "the concept of registering a user and maintaining corresponding information is not a technical problem", nor is "the concept of assigning unique identifiers to entities". Noting that the examining division specifically refers to "concepts" rather than their implementation, the board tends to agree, without however excluding the possibility that a particular combination of such concepts in a computer implementation may increase security and might, for that reason, be found to solve a technical problem. However, in view of the following, a decision of whether or to what extent the contribution to the art made by the claimed method is a technical one is not required.

Claim construction

4. Before the claimed subject-matter can be properly assessed for inventive step, it must be determined how, in the board's view, the skilled person would understand some crucial claim language. Reference is made to claim 1 of the auxiliary request labelled the "seventh" so that all relevant features are considered.

5. Claim 1 concerns a method of registering a user. However, only some of its steps relate to registration in a narrow sense (from the "obtaining" step to the alternatives of "adding" or not "the user to a registration database"), while one claimed step precedes registration ("the user sets an access password [...] before registration takes place" and one is interleaved with

the registration process ("if the method of registering is only partially complete then ... before registration progresses or completes"). For the purpose of assessing inventive step, the board takes all these steps to be part of the claimed method.

6. Claim 1 relates to a method by which, after successful completion, a user (presumably with all data transmitted to the server for that purpose) is added to a "registration database". The claim language does not cover any later use of the mobile application such as the user carrying out a financial transaction on the registered "account". It leaves open whether and how the registered and validated data is used in the process and thus whether and how the security of the process might profit from the validation carried out during registration.

7. Claim 1 specifies that the user sets, in an initial step, a "password" (or such like) which they may have to input when the registration is (interrupted or paused when) "only partially complete" and needs to be continued. Following the appellant's suggestion during oral proceedings, the board takes the relevant claim language to subsume a conventional login procedure. On first use of the mobile application, the user may, for instance, pick a username and a password, which data the user must type in whenever the mobile application is started or restarted. In the board's opinion, the claim language leaves open whether username and password are stored on and validated by the mobile device on its own, or whether the login data is stored on and validated by a remote server.

8. Claim 1 also leaves open from where the mobile application "retrieves" the "data uniquely identifying the

mobile device". The board takes claim 1 to subsume the possibility that the user provides that data. The board notes that this step does not guarantee that the information provided by the user actually identifies the mobile device on which the mobile application is presently run. Also the subsequent "authenticating" step cannot guarantee that: Although the express goal of this step is to "authenticat[e] the user with the mobile device", it is merely defined as "challenging" the user to provide the correct password. The same would be possible if the user identified a different mobile device to which it had access and from it could thus respond to the challenge with the correct password.

9. Claim 1 requires validation of "the user with the account using the data identifying the user, the account data, and the data uniquely identifying the mobile device". The steps of payment and receiving the reference code validate that the user has access to the account. It is undefined in all requests, and unclear, what in this process the data identifying the mobile device is used for, or how. During oral proceedings, the appellant could not provide satisfactory explanation for this issue. The pertinent feature is therefore ignored in the assessment of inventive step.

10. As a summary, the board cannot see that the claim language implies a binding between the account and the mobile device, but rather a registration method during which an account and a mobile device are validated rather independently of each other. In other words, the board considers that the claimed method is insufficient to establish the desired "triangle of trust" and, in particular, to guarantee that the account can only be access by the specific mobile device.

Inventive step
"Fourth" auxiliary request

11. D13 discloses a method of registering a user for a "client application" in which the user inputs personal data and data identifying a mobile device for later use by the application (see in particular paragraph 39, last 7 lines). The applications considered in D13 relate to social networks, but it is specifically indicated that the application may also provide the option for the user to "make purchases" (see paragraph 7).

11.1 From this very generic application, the subject matter of claim 1 differs by the steps of

a) setting of a password on first execution of the application,
b) obtaining from the user (financial) account data),
c) authenticating "the user with the mobile device" indicated via a challenge-response scheme, the expected response being the password,
d) validating, by the server, "the user with the account", and
e) registering the user only if the validation was successful.

11.2 *Re a)* The board considers that it was common-place at the priority date for a user to provide login information to a mobile application when first run and to be challenged for that information whenever the mobile application is started, in particular just before registration (should the user not register directly when the application is first run) and whenever the application is interrupted and needs to continue. The appellant has not challenged this assumption.

11.3 *Re b)* It is obvious in an application such as that of D13 (but also in any mobile banking or e-commerce application, of which many existed before the present priority date), which is meant to support the user in making purchases, that a payment instrument be provided on registration. (Financial) account data is one obvious choice for that.

11.4 *Re c)* In the manner claimed, the authenticating step is indistinguishable from a two-factor authentication, in which a user needs to provide a secret at a particular mobile device (think SMS-TAN or mTAN). Two-factor authentication of this form was well-known in the art at the priority data. Also this assumption was not challenged by the appellant (but see also D2, section "security", page 7, paragraph just below item 6; and D6, section "Two-factor authentication", page 3). It was also commonly known that various codes may be asked for in the process; D6 in particular mentions pseudo-random numbers from a security token, a PIN and a daycode (*loc. cit.*). In view of that, using the (login) password in a two-factor authentication is considered to be obvious.

The appellant insisted that user's response to the challenge must come from the very mobile device running the mobile application. Assuming this were the case (which the board doubts, see above), it would appear to mean that the user would have to provide the password on a mobile device on which they are just using the mobile application. Then, however the claimed challenge-response step boils down to asking the user again for the same password they have just used to log into the mobile application. At best, this seems to be more secure by double checking a secret rather than checking it once. However, the board considers obvious to increase security by repeating security checks.

11.5 *Re d)* The board considers it to be an obvious desirable to validate a payment instrument so as to avoid abuse.

11.6 *Re e)* The board also considers it to be fundamentally obvious, in order to increase data integrity and thus security, to make sure that no incorrect user data is stored on registration, and therefore not to register a user the data of who cannot be validated.

12. In summary, the subject-matter of claim 1 of the "fourth" auxiliary request lacks inventive step over D13 in view of common general knowledge in the art, witness, for example, D2 and D6.

"Fifth" to "seventh" auxiliary request

13. As stated above, the requirement to pass a login procedure whenever a user happens to return to a login-protected application after an interruption is common practice in the art.

14. As the examining division stated, it was known in the art to validate a user account by sending a small payment to the account and requiring the user to provide a "reference" transmitted along with the payment as a proof of (presumably authorized) access to the account. Indeed, D8 uses this scheme (see "Details" under item 1), where the "random amount" acts as the claimed "reference".

15. Accordingly, also claim 1 of the requests labelled "fifth" to "seventh" lacks an inventive step over D13 in view of common knowledge in the art such as D8.

"Eighth" auxiliary request

16. The "eighth" auxiliary request was filed to overcome the board's inventive step objection, in particular insofar as the claimed method of registration does not imply any later use of the data stored in the registration database (see point 6 above).

16.1 The added phrase qualifies that the "adding of the user to the registration database" should be "such that the registered user can engage in peer-to-peer payments and obtain other services using the mobile application and operation of the mobile application on another mobile device for the account is prevented".

16.2 However, the board is unable to see how the storing of user data in the registration database is limited by the intention to use it in "peer-to-peer payments" or "other services", and specifically how the claimed registration method could ensure that the mobile application could not be used on "another mobile device" to access the (financial) account.

16.3 It would appear that the added text constitutes a result to be achieved without any feature which could help achieve it, which makes the added text - and amended claim 1 as a whole - unclear, Article 84 EPC.

16.4 Also, the board does not see how the amendments could help overcome the inventive step objections raised against the higher-ranking requests.

16.5 Therefore, the board does not admit the "eighth" auxiliary request pursuant to Article 13(2) RPBA 2020.

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. Brückner Martin Müller

Decision electronically authenticated