Internal distribution code:

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

Datasheet for the decision of 14 February 2023

Case Number:	T 0663/20 - 3.5.01
Application Number:	12779068.1
Publication Number:	2774098
IPC:	G06Q20/32, G06Q20/40, G06F21/00, G07F7/10, H04W88/06
Language of the proceedings:	EN

Title of invention:
AUTHENTICATION METHOD

Applicant:
Money and Data Protection Lizenz GmbH & Co. KG

Headword:
Authentication method using mobile device/MONEY AND DATA PROTECTION LIZENZ

Relevant legal provisions:
EPC Art. 54, 56, 84
RPBA 2020 Art. 13(2)

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

Keyword:
Novelty - (yes)
Technical effect - improved safety (no - technical, but not verifiable)
Inventive step - reversing communication flow between a user and an authentication entity (yes - non-obvious alternative solution)

Decisions cited:
T 2359/08, T 0520/13, T 1636/18, T 2153/18

Europäisches Patentamt
European Patent Office
Office européen des brevets

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 0663/20 - 3.5.01

DECISION
of Technical Board of Appeal 3.5.01
of 14 February 2023

Appellant: Money and Data Protection Lizenz GmbH & Co. KG
(Applicant) Niederfeldstrasse 19a
33611 Bielefeld (DE)

Representative: Ter Meer Steinmeister & Partner
Patentanwälte mbB
Artur-Ladebeck-Strasse 51
33617 Bielefeld (DE)

Decision under appeal: **Decision of the Examining Division of the European Patent Office posted on 24 October 2019 refusing European patent application No. 12779068.1 pursuant to Article 97(2) EPC.**

Composition of the Board:

Chairman W. Chandler
Members: R. Moser
L. Basterreix

Summary of Facts and Submissions

I. This case concerns the applicant's appeal against the decision of the examining division to refuse the European patent application No. 12779068.1.

II. The examining division found that claim 1 of the main request was not novel over D1 (WO 2008/052592 A1). Additionally, even if the claim were deemed to be novel, it would still be obvious as it merely proposed an alternative solution for storing data.

For the auxiliary request, the examining division raised objections on the grounds of lack of clarity and added subject-matter. Moreover, they concluded that claim 1 did not involve an inventive step over D1 or D13 (WO 2010/086608 A2).

III. In the statement setting out the grounds of appeal, the appellant requested that the decision of the examining division be set aside and that a patent be granted on the basis of the refused main request or a newly filed auxiliary request.

IV. In the communication accompanying the summons to oral proceedings, the Board tended to agree with the appellant that the claimed subject-matter appeared to be novel over D1.

However, the Board remained unconvinced that the distinguishing features resulted in a technical effect that was related to the security of the authentication process. Rather, the Board tended to regard these features as offering an obvious alternative solution that would have been chosen based on non-technical factors, such as user preferences.

V. In a letter dated 15 December 2022, the appellant submitted further arguments in favour of inventive step, in particular that the inventive method, unlike D1, was not vulnerable to SMS-spoofing attacks.

VI. During the oral proceedings before the Board on 14 February 2023, which took place by videoconference, the appellant filed a new main request replacing all previous requests.

The appellant's final request was thus that a patent be granted on the basis of the main request filed during the oral proceedings before the Board.

At the end of the oral proceedings the Chairman announced the Board's decision.

VII. Claim 1 of the main request reads:

"A method of authenticating a user to a transaction at a terminal (10), the method comprising the following steps:

- a user identification is transmitted from the terminal (10) to a transaction partner (12) via a first communication channel (14),
- the transaction partner (12) forwards the user identification to an authentication device (18),
- using a second communication channel (20), which involves a mobile communications network, in conjunction with a mobile device (16) of the user for checking an authentication function, which is normally inactive and is activated by the user only preliminarily for the transaction,
- as a criterion for deciding whether the

authentication to the transaction shall be granted or denied, the authentication device (18) checks whether a predetermined time relation exists between the transmission of the user identification and an active state of the authentication function, and,

- if said criterion for granting the authentication is fulfilled, the authentication device (18) sends an authentication signal to the transaction partner,

characterized

in that the authentication function is implemented in the mobile device (16) of the user and permits the authentication device to detect, via the second communication channel (20), whether or not the authentication function is active, and in that, based on the user identification, the authentication device (18) directly contacts the mobile device to check the active state of the authentication function and, if the authentication function is active, the authentication device (18) receives a response from the mobile device via the second communication channel, said response including the information that the authentication function is active, and,

- wherein the authentication function is automatically deactivated after a predetermined time interval after its activation and/or when its active state has been checked."

VIII. Claim 11 reads:

"A mobile device (16) for use in the authentication method according to any of the claims 1 to 6, comprising a wireless transceiver (40), an ON-switch (48) and an electronic controller (44) that implements said authentication function and is configured to activate the authentication function in response to the ON-switch (48) being operated and to deactivate the same after it has been active for a predetermined time interval or after its state has been checked."

Reasons for the Decision

The invention

1. The invention relates to a method for authenticating a user, such as when making a payment at a supermarket's point-of-sale (POS) terminal. Methods that allow users to authenticate themselves using their mobile phones are known in the art such as D1.

The purpose of the invention is to provide an easy authentication method that uses a mobile device with low complexity, while at the same time ensuring a high level of security - see page 2, lines 11 and 12, and page 3, lines 12 to 14 of the published application.

2. As shown in Figure 1, the POS terminal 10 sends the user's ID to a bank 12 during the payment process (first step of the preamble in claim 1). The bank then forwards the ID to a trusted third party 18 (second step).

Based on this information, the trusted third party checks if the user has activated an authentication function on his mobile device 16. If the user has activated this function, the trusted third party informs the bank accordingly, allowing the transaction to be approved (third and fourth steps).

3. The main concept is that the trusted third party obtains the status of the authentication function by *querying the mobile device* (first feature of the characterising part).

Novelty and clarity

4. It is common ground that D1 discloses authenticating a user to a transaction involving a mobile device, a terminal, a bank and an authentication device with a trusted third party. The authentication further involves temporarily activating an item for the duration of the transaction. In D1 this item is status information in the database at the authentication device set by an authentication message from the user (in the form of an SMS) to the Application Server - as illustrated in Figure 3 of D1.

5. In the invention the item is set by the user in the mobile device and is queried by the authentication device. However, the refused claim language, particularly the phrasing "the authentication device (18) contacts [an] address of the mobile device" and "receives a response from the second communication channel", was unclear. This could have been the reason that the examining division interpretated this feature as a Home Location Register (HLR) lookup. In this scenario, the trusted third party (authentication device) queries the HLR database to verify the status of the authentication function, which indicates whether or not the mobile device is connected to the network (as explained in page 4, lines 1 to 8).

The examining division then mapped this feature to the database update carried out by the trusted third party (Application Server) in D1 (as described at page 12, lines 28 to 35). As a result, they concluded that both in D1 and in the claim there was no direct communication between the trusted third party and the user's mobile device and, as a result, that claim 1 was not new.

6. In its preliminary opinion, the Board considered that, despite its ambiguity, the claim must imply that the authentication device initiates communication with the mobile device, as mentioned above at points 2 and 3.

7. In addition to the above mentioned feature, the Board also raised clarity issues against the following features of claim 1 of the refused main request during the oral proceedings:

- "and a second communication channel (20)"

The claim defines a method, however, this feature is more related to a component of a system.

- "and the authentication function is automatically deactivated"

The Board observed that the claim did not indicate when and under what conditions the authentication function was deactivated (as shown in page 8, lines 15 to 26).

Moreover, it was unclear how this related to the "predetermined time relation" requirement, which the Board believed could only mean verifying whether the authentication function was active.

8. In response to these objections, the appellant submitted a new main request. The Board, exercising its discretion under Rule 13(2) RPBA, admitted the request

since it was submitted in response to new objections.

The amendments adequately address the issues mentioned by the Board. In particular, they clarify the distinguishing feature by specifying that the authentication device "**directly** contacts **the mobile device**" and "receives a response **from the mobile device** via the second communication channel" (emphasis added by the Board).

The Board judges that amended claim 1 is clear (Article 84 EPC) and avoids the examining division's interpretation that the authentication device does not initiate communication with the mobile device, but with the HLR, and is thus novel over D1 (Article 54 EPC).

9. Fundamentally, claim 1 differs from D1 in terms of a reversed communication flow which is conveyed through the following feature:

"the authentication device (18) directly contacts the mobile device to check the active state of the authentication function and, if the authentication function is active, the authentication device (18) receives a response from the mobile device via the second communication channel".

In other words, the trusted third party follows the principle of "don't call us, we'll call you".

Inventive step

10. As mentioned earlier (see point 1), the invention aims to provide authentication with a high level of security.

Accordingly, the appellant formulated the technical problem as further improving the safety of the authentication process.

11. The appellant argued that, unlike in D1, the authentication process in the invention was simpler and more convenient for the user. The user only had to activate the authentication function, for example, by pressing the ON-switch 48 on a mobile device 16 as shown in Figure 7. This was especially beneficial in stressful situations such as paying at a POS terminal.

Moreover, the invention required a device of low complexity because there was no need for elaborate input means to enter the user's identification or card information, which was necessary in D1.

12. The appellant also contended that the invention was not vulnerable to SMS-spoofing attacks, unlike D1.

Since no message containing sensitive information was transmitted from the mobile device to the authentication device, it was impossible for a fraudster to intercept the message, replicate the user's phone number, and successfully authenticate.

Additionally, if one were to start with D1, an obvious solution would have been to incorporate encryption or filters to identify spoofing attempts.

13. The appellant argued that there was another distinguishing feature, which was that the activation function status was stored in the mobile device, not in the authentication device.

The appellant believed that starting from D1, storing the enablement status of the user's cards on the phone would not have made sense. According to the teaching of D1, this would have increased the number of message exchanges between the phone and the Application Server. This was considered a technical prejudice for the skilled person and could only have been overcome in a non-obvious manner.

14. To sum up, the appellant argued that D1 did not suggest reversing the communication flow, nor was this an obvious solution in 2011, the priority date of the application. Furthermore, the simple and secure solution of claim 1 was a strong indication of an inventive step.

15. The Board does not consider that inventive step can be based on the effect of improved safety, as it is not convinced that this effect is actually achieved.

Firstly, D1 discloses data transmission methods that are impervious to (SMS-)spoofing attacks, such as a secure IP channel (page 3, lines 27 to 34) or a web application (fourth embodiment on page 21, line 30 *et seq.*). If these embodiments of D1 are chosen as starting points, the aforementioned effect cannot be attained. Furthermore, the invention provides limited and potentially conflicting details concerning the data transmission process. Page 10, lines 21 to 29, mentions an applet that either responds to a request from the authentication device or sends a request, with the second option appearing to conflict with claim 1.

Secondly, the Board considers that if the aforementioned effect were actually achieved, it would directly result from the communication flow, which involves the trusted third party requesting authentication from the user. This also implies where the authentication status data is stored - clearly, if the user is asked whether he wants to authenticate the transaction, he must possess this information.

16. A key question is whether the reversal of the communication flow is motivated by non-technical considerations. If so, according to the COMVIK approach, it can be included in the problem formulation. In this case, the skilled person would have arrived at the invention in an obvious way. Essentially, he would only need to reverse the "Change Status Request" step in D1, as shown in Figure 3.

In its preliminary opinion, the Board had tended to consider that the reversal of the communication flow was motivated by non-technical considerations, such as user convenience.

17. During the oral proceedings, however, it became apparent that there was no reason for the user to request a reversal of the communication flow.

Both in D1 and in the invention, when waiting at the POS, the user only needs to press a button and perhaps input some data to initiate payment authentication. What occurs next, such as sending an authentication message or activating an authentication function, no longer concerns the user. Thus, these aspects cannot be considered to be part of a non-technical requirement, such as a user preference, under the COMVIK approach. Rather, it is part of the technical implementation that is handled by a technically skilled person.

18. Therefore, and given that there is no obvious advantage of the invention starting from D1, the objective

technical problem that the reversal of the communication flow solves can be formulated as providing an alternative method of authentication to the one known from D1.

19. While the choice of where to perform the authentication may appear straightforward, the Board is disinclined to simply assert that the invention is obvious.

Firstly, there is no indication, hint, or necessity in D1 to reverse the communication flow. Doing so could result in certain drawbacks, such as the user becoming unreachable if he moves to an area with no network connection, or the authentication process taking longer. Furthermore, the fact that in D1 the trusted third party manages the status of card data (see e.g. page 11, lines 24 to 35) rather teaches away from the invention. There is no need for the trusted third party to ask the user upon receiving a transaction request, as it would suffice to check the status database.

Secondly, while a solution may be considered obvious if it is an equally well known alternative, the Board finds no example in the prior art of its use for authenticating a user transaction at a terminal, let alone any evidence to show that the skilled person would have applied this principle to the method in D1. While this may be conceivable in hindsight, there is no obvious inspiration for the skilled person to do so.

Occasionally, obvious solutions can be derived from the skilled person's appreciation of an expected trade-off of some aspect of the system's performance. Some previous examples in cases from this Board show the idea:

Case	***Alternatives***	***Trade-off***
T 2359/08	returning pages after clicking on the embedded links / already with the retrieved document	amount of data transmitted / speed required to access the data pages of the embedded links
T 520/13	process data locally / centrally	latency / storage space and processing capabilities
T 1636/18	implement functionality on the client device / server	network bandwidth / available computational resources
T 2153/18	providing data to the client on request / pre-fetching potentially relevant information	bandwidth and computational requirements / query response time

However what these cases appear to have in common is that the trade-off is what could be termed "one-dimensional" in that the location or timing of some part of the functionality changes, but the system functions in essentially the same way.

For example, in T 1636/18 - *Estimating departure time/ QUALCOMM*, the functionality of various features was specified as being performed in either the client or the server, but nothing else was changed. In T 520/13 - *Advertisement selection / MICROSOFT*, part of the process of selecting an advertisement was shifted to the client, but the selection process was otherwise unchanged.

In the Board's view, the solution in the present case differs from these examples in that it has an additional "dimension". Not only is the authentication performed on a different device, but the communication flow is different and the user no longer needs to send a message to the server. Although it could be argued that these are obvious corresponding modifications, the Board considers that juggling this extra dimension takes the present case out of the realm of a straightforward trade-off, somewhat like choosing from two lists does for novelty. In such a situation it is not immediately apparent what is being traded off and how. Thus, again, the Board considers that some further motivation would be required.

Accordingly, the Board judges that the subject-matter of claim 1 involves an inventive step (Article 56 EPC).

20. The subject-matter of claim 11 involves an inventive step for the same reasons.

Order

For these reasons it is decided that:

1. The decision under appeal is set aside.

2. The case is remitted to the department of first instance with the order to grant a patent on the basis of the set of claims 1 to 12 filed during the oral proceedings and a description to be adapted.

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

T. Buschek W. Chandler

Decision electronically authenticated