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 20 July 2023

Case Number:	T 2192/18 - 3.5.01
Application Number:	07815833.4
Publication Number:	2080158
IPC:	G06Q20/00
Language of the proceedings:	EN

Title of invention:
A SYSTEM AND METHOD FOR VERIFYING A USER'S IDENTITY IN ELECTRONIC TRANSACTIONS

Applicant:
Scammell, Dan

Headword:
User identity verification/SCAMMELL

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

Keyword:
Inventive step - performing user authentication by a separate computer (no - obvious alternative)

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

Decisions cited:

T 0520/13, T 1463/11, T 2251/13

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

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 2192/18 - 3.5.01

DECISION
of Technical Board of Appeal 3.5.01
of 20 July 2023

Appellant:
(Applicant)

Scammell, Dan
1729 Hampton Drive
Coquitlam, BC V3E 3C9 (CA)

Representative:

Haseltine Lake Kempner LLP
One Portwall Square
Portwall Lane
Bristol BS1 6BH (GB)

Decision under appeal:

Decision of the Examining Division of the European Patent Office posted on 13 April 2018 refusing European patent application No. 07815833.4 pursuant to Article 97(2) EPC.

Composition of the Board:

Chairman W. Chandler
Members: I. Kürten
E. Mille

Summary of Facts and Submissions

I. This appeal is against the decision of the examining division to refuse the European patent application No. 07815833.4 for lack of inventive step (Article 56 EPC) over D1 (WO 2005/001670 A2). The examining division essentially held that the differences related to non-technical requirements or straightforward design choices.

1.1 In the statement setting out the grounds of appeal, the appellant requested that the decision to refuse the application be set aside and that a patent be granted on the basis of a new request essentially corresponding to the refused request.

1.2 The Board scheduled oral proceedings for 6 October 2022. In the communication accompanying the summons, the Board set out its provisional opinion that the claimed method comprised fewer differences than the examining division had identified. The Board tended to agree with the finding of a lack of inventive step.

1.3 With a reply dated 6 September 2022, the appellant filed a new sole request and submitted supporting inventive step arguments.

1.4 In a letter dated 15 September 2022, the appellant requested postponement of the oral proceedings. The Board acceded to the request for postponement and rescheduled the oral proceedings.

1.5 With a letter dated 20 June 2023, the appellant filed another new sole request.

1.6 During the oral proceedings, held on 20 July 2023 by videoconference, the appellant confirmed the request filed in writing.

1.7 Claim 1 of the appellant's sole request reads:

A user identity verification method for verifying the identity of a user (101) by a verifier (301) in the course of an electronic transaction, said user identity verification method comprising the steps of:

(a) sending (702), by a verification requestor (201) a verification initiating request to the verifier (301);

(b) upon receiving the verification initiating request, retrieving by the verifier (301) a user access number for a user communications device (2303);

(c) establishing communications (1503) between the verifier (301) and the user communications device (2303) by using the user access number retrieved at Step (b);

(d) sending an identity verification request (IVR) from the verifier (301) to the user communications device (2303) through communications (1503) established at Step (c);

(e) inputting (1802) by the user (101) a putative secure identifier;

(f) sending (1602) to the verifier through communications (1503) established at Step (c) a response to the IVR of Step (d);

(g) retrieving a bona fide secure identifier by the verifier (301);

(h) comparing (1502) the putative secure identifier input at Step (e) with the bona fide secure identifier retrieved at Step (g);

(i) communicating (2402, 2302) the result of the comparison of Step (h) to the verification requestor (201), to verify the identity of the user (101) to the verification requestor 201); and

(j) the verification requestor (201) allowing the transaction to proceed only if the comparison of Step (h) results in a match between the putative secure identifier and the bona fide secure identifier;

wherein:
said communications between the verifier (301) and the user communications device (2303) are conducted over a communications link (1503) between a first verifier communications device (2403) of the verifier (301) and the user communications device (2303), opened by the verifier (301) based on the user access number;

said verification initiation request is sent from the verification requestor (201) to the verifier (301) through a communications link (1803) between the verification requestor (201) and a second verifier communications device (803) of the verifier (301);
characterised in that:

the verification requestor (201) is an entity, or group of entities that interact, for providing financial services related to the transaction;

the verifier (301) is a distinct entity from the verification requestor;

and in that the method further comprises:

(k) pre-enrolling the user (101) with the verifier, comprising the steps of:

(k1) assigning to the user (101) the bona fide secure identifier; and
(k2) storing the bona fide secure identifier in a verifier database (701) that is directly accessible only by the verifier (301);

(l) pre-enrolling the user communications device (2303) with the verifier, wherein pre-enrolling the user communications device comprises the steps of:
(l1) obtaining the user access number for the user communications device (2303), wherein the user access number can be used to open a communications link with the user communications device (2303); and,
(l2) storing the user access number in the verifier database (701); and

(m) pre-enrolling an account of the user, wherein pre-enrolling the account comprises setting a flag, at the verification requestor, that indicates whether or not Steps (a) through (h) and (i) through (j) are to be performed.

Reasons for the Decision

2. Admittance (Article 13(2) RPBA)

The Board admitted the request filed on 20 June 2023 into the proceedings under Article 13(2) RPBA. This request only corrects minor typographical errors in the earlier request filed with the letter of 6 September 2022. The latter was a genuine attempt to address the Board's new objections raised in the communication accompanying the summons. These objections resulted from a new interpretation of claim 1 and a new feature mapping to D1, which differed from those in the decision under appeal.

3. The invention

3.1 The invention concerns authenticating a person who initiates an electronic transaction, e.g. by using a credit card to pay for purchased goods (page 1, first paragraph of the published application). The main idea is to send a request to the legitimate cardholder's mobile phone to input a password and to compare this password to a pre-stored bona fide password (paragraph bridging pages 6 and 7).

3.2 In a preliminary phase (Figure 1), the user and the user's mobile phone ("user communications device" in claim 1) are enrolled by obtaining and storing the bona fide password ("bona fide secure identifier") and the user's mobile phone number ("user access number") in a database (steps (k), (l) in claim 1).

3.3 The authentication process is illustrated in Figure 3. When the user initiates a transaction at a point-of-sale (POS) terminal, the POS sends a transaction request to bank 303 ("verification requestor"). If the user's account has been flagged for identity verification (step (m)), the bank sends an identity verification request to a verifier 203 (step (a)). The verifier retrieves the stored mobile phone number from the database 703 and sends the identity verification request to the user's mobile phone 2303 (steps (b) to (d)). The user responds by entering a password ("putative secure identifier"), which the verifier compares to the stored bona fide password (steps (e) to (h)). The verification result is sent to the bank, and if it is positive, the transaction is processed (steps (i), (j)).

The verifier has two communications devices 803 and 2403 (e.g. two transceivers) for the separate communications links 1803 and 1503 with the bank 303 and the user's mobile phone 2303, respectively (last two features in the preamble).

4. Claim interpretation and novelty

4.1 It is common ground that D1, like the claimed invention, discloses a two-factor user authentication in the context of electronic transactions. In both cases, a verification entity receives an authentication request and forwards it to the user's mobile phone. The user enters a PIN/password, which the verification entity compares to a previously stored PIN/password. If there is a match, the transaction is processed (D1, page 13, line 14 to page 14, line 26). While D1 does not explicitly disclose an enrollment phase, the Board considers it to be implied since the user's PIN and mobile phone number must have been obtained and stored beforehand.

4.2 The main difference lies in the entities that send and process the authentication request. In Figure 8 of D1, the entity sending the request is a "transaction processing client", such as a POS, and the entity processing the request is a "transaction processing server", which is part of the financial services provider network. In claim 1, the request is sent by a "verification requestor" and processed by a "verifier". Although not explicitly stated in claim 1, the Board interprets these two terms to refer to computing devices, as defined in the corresponding independent system claim 15.

4.3 In its preliminary opinion, the Board mapped the "verification requestor" in claim 1 to the "transaction processing client" and the "verifier" to the "transaction processing server". Amended claim 1, however, defines the "verification requestor" as "an entity, or group of entities that interact, for providing financial services related to the transaction". In view of this, the Board interprets the "verification requestor" as the bank's computer, which aligns with the examining division's interpretation. This means that the "verification requestor" can no longer be mapped to the transaction processing client in D1.

Nonetheless, in D1, the transaction processing client sends a transaction authorisation request to the transaction processing server, which first checks whether the transaction is financially permissible before calling a separate transaction authorisation component to perform the two-factor authentication (see e.g. page 12, lines 5 to 24 and page 13, lines 5 to 16). This implies that the server sends a request to this component to perform the authentication. In other words, the transaction processing server in D1 both sends and processes the authentication request.

4.4 Hence, claim 1 differs in that the sending and processing of the authentication request are carried out by separate computers. The bank's computer (the "verification requestor") sends the authentication request to the "verifier", which performs the two-factor authentication and returns the result. A further difference is that the bank's computer sends this request only if the user's account has been flagged for verification. Furthermore, the "verifier" has its own database that stores the user's mobile phone number and password, whereas in D1 these data are stored in the bank's databases.

5. Inventive step

5.1 The examining division held that outsourcing the user identity verification to a separate verifier was a non-technical requirement and that the skilled person would have arrived at the claimed technical implementation in an obvious manner. In an alternative line of reasoning, they stated that even if the separate verifier was based on technical considerations, this would have been a straightforward design choice for the skilled person.

5.2 The Board agrees that outsourcing purely commercial transactions might indeed be driven by non-technical considerations. However, in this case it could be argued that the verifier in claim 1 implements a technical authentication process involving technical aspects related to the verifier's communication with the user's phone and the bank's computer. Hence, the Board can accept that the decision to carry out the two-factor authentication on a separate computer is a technical one and should be examined for obviousness (see e.g. T 1463/11 - *Universal merchant platform/ CardinalCommerce*, points 19 to 21).

On the other hand, flagging accounts for identity verification is an administrative requirement, reflecting subjective preferences of the users or the bank. This requirement does not enter the assessment of inventive step.

5.3 The key question is then whether the technically skilled person, starting from D1, would have considered implementing the two-factor authentication on a separate computer. The Board considers this to be the case for the following reasons:

5.4 Firstly, D1 hints at this alternative in Figure 3, which shows the two-factor authentication as an add-on to an existing transaction processing system on a separate server. Although not discussed explicitly, the drawing itself suggests to the skilled person that using a separate server is a viable option.

5.5 Secondly, the Board agrees with the examining division that the choice of whether to implement distinct functionalities on separate computers or a single computer is a matter of routine design. It involves considering well-known trade-offs between factors like latency, security, and flexibility. A single computer reduces latency and might be less susceptible to security breaches, such as "man in the middle" attacks, but it is less flexible for modifications and upgrades. The Board considers that the decision to carry out the two-factor authentication on a separate verifier is a simple appreciation of such trade-offs (see, e.g. T 520/13 - *Advertisement selection/MICROSOFT*, point 3.4).

The Board acknowledges that a known alternative may become non-obvious in certain circumstances. For instance, this might be the case if technical prejudices against this alternative prevail (e.g. T 1463/11, *supra*, point 30), or if neither the cited prior art nor the skilled person's common general knowledge provides an incentive for using this alternative in the context of the invention (e.g.

T 2251/13 - *Projection surface with built-in track pad/ ORDAMO*, point 3.5).

However, the Board sees no such circumstances in the present case. The description of the application also supports this view, as it presents the implementation of the two-factor authentication on a separate verifier and the bank's computer as equivalent alternatives, without highlighting any specific advantages of either option (see, in particular, page 2, lines 20 to 30 and page 16, lines 6 to 9).

5.6 The appellant argued that using a separate verifier for the two-factor authentication went beyond a mere separation since it enhanced the security of the transaction processing. There were two main reasons for this:

Firstly, neither the bank nor the verifier had access to all data needed to authenticate a fraudulent transaction. The user's phone number and password were stored only in the verifier's database, which was inaccessible to the bank. Conversely, the verifier lacked access to the user's identity and bank account(s), which were stored only in the bank's computer.

Secondly, the communications between the bank and the verifier, as well as between the verifier and the user's phone, were uni-directional and the sessions were closed after each communication. This made it difficult for a malicious attacker to capture and misuse data from previous sessions. As a result, the risk of man-in-the-middle attacks, which was a major concern at the time, was effectively eliminated.

5.7 The Board does not find these arguments convincing:

Firstly, claim 1 only specifies that the user's phone number and password are stored in a "verifier database", which is "directly accessible only by the verifier". This does not exclude the possibility of the bank having indirect access to this database through the verifier or storing a copy of these data. Likewise, the claim does not rule out the verifier storing a copy of the user's identity and accounts or having access to the bank's database.

Secondly, the entire application is silent about uni-directional communications and session closures after each communication. On the contrary, according to steps (c), (d), and (f) in claim 1, the verification request from the verifier to the user's device and the response are sent within the same communication session. The appellant's argument that the uni-directional arrows in Figure 3 imply uni-directional communications is not convincing because the figure alone does not unambiguously define the arrows' meaning. If it did, the same interpretation would apply to Figure 3 of D1, which also shows uni-directional arrows between the existing bank process and the authentication server, and between the server and the user's phone.

5.8 The appellant further argued that the invention's commercial success demonstrated its inventiveness.

The Board is not convinced because there is no evidence linking this success to the differences over D1. The commercial success could have been influenced by other aspects of the commercial product not claimed or disclosed in the application, or it might have been the result of effective marketing strategies and selling techniques.

5.9 Having decided to implement the two-factor authentication on a separate computer (the verifier), the skilled person would have to provide means for communication between the bank's computer and the verifier. Given D1's teaching that the transaction initiation and authentication are carried out on separate communication streams, using e.g. fixed-line and GSM networks (e.g. page 2, lines 11 to 13), it would be obvious to equip the verifier with two separate communication devices - one for communicating with the user's phone and another for communicating with the bank's computer. Furthermore, since each computer operates on a distinct data subset, it would be obvious for the skilled person to segregate the data in the bank's databases of D1 into two databases, based on the respective functions of each computer. Hence, the skilled person would arrive at the claimed invention in an obvious manner.

5.10 In view of the above, the Board judges that claim 1 of the appellant's sole request does not involve an inventive step (Article 56 EPC).

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 ✦

S. Sánchez Chiquero W. Chandler

Decision electronically authenticated