Internal distribution code:

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

Datasheet for the decision of 21 April 2023

Case Number: T 1772/20 - 3.5.03

Application Number: 06820602.8

Publication Number: 1969880

IPC: H04W12/06, H04L29/06

Language of the proceedings: EN

Title of invention:
System and method for dynamic multifactor authentication

Patent Proprietor:
OneSpan International GmbH

Opponents:
KOBIL GmbH
Thales Dis France SA
Molnia, David

Headword:
Dynamic multifactor authentication/ONESPAN

Relevant legal provisions:
EPC Art. 116(1), 123(2)
RPBA 2020 Art. 12(8)

Keyword:
Decision in written proceedings - (yes): withdrawal of request for oral proceedings - oral proceedings neither necessary nor expedient
Added subject-matter - main and auxiliary requests (yes)

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 1772/20 - 3.5.03

D E C I S I O N
of Technical Board of Appeal 3.5.03
of 21 April 2023

Appellant: (Opponent 1)	KOBIL GmbH Pfortenring 11 67547 Worms (DE)
Representative:	Cohausz & Florack Patent- & Rechtsanwälte Partnerschaftsgesellschaft mbB Bleichstraße 14 40211 Düsseldorf (DE)
Respondent: (Patent Proprietor)	OneSpan International GmbH World-Wide Business Center Balz-Zimmermannstrasse 7 8152 Glattbrugg (CH)
Representative:	Beck, Michaël Andries T. IPLodge Technologielaan 9 3001 Heverlee (BE)
Party as of right: (Opponent 2)	Thales Dis France SA 6, rue de la Verrerie 92190 Meudon (FR)
Representative:	Körfer, Thomas Mitscherlich PartmbB Patent- und Rechtsanwälte Sonnenstrasse 33 80331 München (DE)
Party as of right: (Opponent 3)	Molnia, David df-mp Dörries Frank-Molnia & Pohlman Patentanwälte Rechtsanwälte PartG mbB Theatinerstrasse 16 80333 München (DE)

Representative: Molnia, David
Df-mp Dörries Frank-Molnia & Pohlman
Patentanwälte Rechtsanwälte PartG mbB
Theatinerstrasse 16
80333 München (DE)

Decision under appeal: **Interlocutory decision of the Opposition Division of the European Patent Office posted on 26 June 2020 concerning maintenance of the European Patent No. 1969880 in amended form.**

Composition of the Board:

Chair K. Bengi-Akyürek
Members: K. Peirs
C. Heath

Summary of Facts and Submissions

I. The appeal lies from the interlocutory decision of the opposition division to maintain the opposed patent (hereinafter: "the patent") in amended form on the basis of the proprietor's "Auxiliary Request 1". The proprietor's main request (labelled "Auxiliary Request 4" in Reasons 2.1 of the appealed decision) was deemed not to be allowable for lack of an inventive step (Article 56 EPC).

II. The substantive requests of the parties are as follows:

- The appellant (opponent; labelled "OP1" in the impugned decision) requested that the appealed decision be set aside and that the patent be revoked.

- The respondent (proprietor) requested with the written reply to the appeal as a **main request** that the appeal be dismissed, i.e. that the patent is upheld as maintained by the opposition division. In the alternative, the respondent requested that the patent be maintained in amended form on the basis of an **auxiliary request**. This auxiliary request is identical to "Auxiliary Request 2" filed during the oral proceedings before the opposition division on 20 January 2020 (cf. point 1.36 of the "Summary of facts and submissions" and Reasons 2.3 of the appealed decision).

III. The parties were summoned to oral proceedings before the board. A communication was issued under Article 15(1) RPBA 2020 including the board's negative preliminary opinion as concerning added subject-matter

(Article 123(2) EPC).

IV. In a written reply, the respondent withdrew its request for oral proceedings and indicated that it would not be attending the arranged oral proceedings.

V. Subsequently, the oral proceedings were cancelled.

VI. Claim 1 of the **main request**, i.e. claim 1 as maintained by the opposition division, reads as follows (board's feature labelling):

(a) "A method of authenticating a user (1), the method comprising the steps of:
(b) - sending an authentication request to a remote authentication device (3);
(c) - generating a first piece of authentication information;
(d) - generating, within the mobile device of the user, a second piece of authentication information which is at least partially based on the received first piece of authentication information;
(e) - sending the second piece of authentication information to the remote authentication device;
(f) - validating the second piece of authentication information;
(g) and, if the second piece of authentication information is successfully validated,
- generating an authentication signal;
(h) wherein the first piece of authentication information is received at the mobile device (2) from an access terminal (4);
(i) characterised in that the first piece of authentication information is presented as an image on a display means of the access terminal (4) and

captured therefrom using a digital camera of the mobile device (2);

(j) the authentication request comprises personal information of the user (1) and transactional information related to a transaction which the user (1) wishes to make;

(k) the first piece of authentication information contains the transactional information related to the transaction which the user (1) wishes to make; and

(l) the second piece of authentication information comprises a signature over a message contained in the first piece of authentication information,

(m) wherein the message contained in the first piece of authentication information is displayed to the user, and the signature is generated if the transaction is accepted by the user; and

(n) wherein the step of generating the second piece of authentication information is done using the International Mobile Equipment Identity, IMEI, information relating to the Subscriber Identity Module, SIM, or any other information specific to the mobile device (2) of the user (1);

(o) wherein the step of sending the second piece of authentication information to the remote authentication device is done by the mobile device; and

(p) wherein the step of validating the second piece of authentication information comprises:

- receiving from the mobile device (2) information relating to the location of the mobile device (2);

(q) - receiving from the access terminal (4) information relating to the location of the access terminal (4);

(r) - comparing the location of the mobile device with the location of the access terminal; and
(s) - validating the second piece of authentication information only if the location of the mobile device matches the location of the access terminal".

VII. Claim 1 of the **auxiliary request** includes all the features of claim 1 of the main request, with the word "and" removed from feature (o), and further includes, at the end, the following feature:

(t) "wherein the authentication device (3) uses information contained in an Internet Protocol packet header to determine the Internet Protocol address of the access terminal (4), with which information the authentication device (3) determines the location of the access terminal (4)".

Reasons for the Decision

1. *Decision in written proceedings*

1.1 After the parties were summoned to oral proceedings, the respondent withdrew its request for oral proceedings (see point IV above), thereby obviating the need for oral proceedings.

1.2 Given that the board does not consider the conduct of oral proceedings to be expedient either (cf. Article 116(1) EPC), the decision is handed down in written proceedings (Article 12(8) RPBA 2020).

2. *Technical background*

The invention underlying the opposed patent relates to authenticating a user within the framework of performing a banking or commercial transaction. Such transactions are prone to several kinds of attacks, such as phishing. The patent adopts in this respect a "dynamic multifactor authentication". From the authentication factors underlying this authentication, a first one can be entered manually in the form of an account name and password. A second authentication factor is then sent automatically to a mobile device via Bluetooth or SMS or semi-automatically via a mobile phone's camera.

The fact that the "second authentication factor" is entered into the mobile device (semi-)automatically is used by the system according to the invention to generate messages with allegedly "longer codes" and "a greater amount of transactional information". By doing so, the invention is stated to provide for an increased security and usability. It thereby relies on the ever increasing processing power of mobile devices.

3. *Main request: claim 1 - added subject-matter*

Claim 1 of the **main request** is related to original claims 1, 3, 7, 10 to 12 and 15. Nonetheless, it comprises added subject-matter at least due to the amendments underlying **features (j), (k) and (m)**:

3.1 **Feature (j)** has no direct and unambiguous disclosure in the application as filed for the following reasons.

3.1.1 First, the original application's "personal information" only concerns data which the user enters

into the access terminal (see page 9, lines 17 to 19 and page 11, lines 5 to 7, both of the application as filed). By contrast, the "personal information" of feature (j) is not restricted in this regard. Within the context of secure web-based transactions, it could, for instance, relate to the user's favourite dish from a particular restaurant as stored in a web-browser's cookie. Alternatively, it can relate to the user's gender or blood type as apparent from their online medical file. As a further alternative, it can relate to the user's mobile phone number or finger print to just name a few examples. None of these examples are however necessarily entered by the user into the access terminal, such as the "Point of Sales" terminal considered at lines 6 and 7 of page 8 as filed. The fact that the application as filed did not impart a special meaning to the entering of the personal data by the user into the access terminal does not mean that there is a direct and an unambiguous disclosure for the general "personal information" according to feature (j).

3.1.2 Moreover, features (a) to (s) are also silent about the use or purpose of the "personal information" of feature (j). This use or purpose could be, for instance, presenting the user with dedicated information based on the personal information. Conversely, the appellant correctly pointed out that the application as filed only uses this personal information for validation by remote authentication device 3 (see page 9, lines 20 to 24 and page 11, lines 7 to 13 as filed).

3.2 Regarding **feature (k)**, the introduction of the definite article before "transactional information" implies that the first piece of information according to

features (i) and (k) comprises the same "transactional information" as the "authentication request" of feature (j). The appellant correctly observed that this is not directly and unambiguously disclosed.

The last paragraph of Reasons 2.1.1.2 of the appealed decision relies on page 9, lines 20 to 23, 29 and 30 as filed and indicates that the skilled reader, when "reading the passage as a whole", would have understood that "the transaction information is the same". Even if one understands the term "information pertaining to the specific transaction which the user 1 wishes to perform" used at page 9, lines 22 and 23 as filed to be equivalent to the term "transactional information" used at page 9, line 29 as filed, there is no direct and unambiguous disclosure that the former is sent "via the authentication request", contrary to what the Reasons of the appealed decision state. In particular, the preposition "along with" of page 9, line 22 as filed does not imply that the "personal information" and the "information pertaining to the specific transaction which the user 1 wishes to perform" are sent as one request.

3.3 Regarding **feature (m)**, the phrase "the signature is generated if the transaction is accepted by the user" has no direct and unambiguous disclosure in the application as filed. At page 12, lines 13 and 14 as filed, it is merely stated that the message is signed if the transaction is accepted by the user. It is however not stated there that the user's signature is generated at that very point in time. This signature could e.g. have been generated beforehand and then stored on mobile device 2. Moreover, the appellant correctly observed that feature (m) does not specify the unit by which the signing is actually performed. By

contrast, page 12, lines 12 to 16 as filed suggests this unit to be the mobile device 2. This amounts to an unallowable intermediate generalisation.

The board also agrees with the appellant that features (a) to (s) are silent about the case where the user does not accept the transaction. Page 12, lines 17 to 23 as filed in fact states that in this case "*the encoded and encrypted message is sent to the remote authentication device 3 without being digitally signed*". Alternatively, "*the encrypted message could not be sent at all*". Contrary to what is suggested by the respondent, the skilled reader would, based solely on features (a) to (s), indeed be immediately aware of more than just the two possibilities as disclosed in the application as filed. A third possibility which is not present in the application's original disclosure is, for instance, that a warning is shown to the user requesting confirmation by the user not to accept the transaction.

3.4 Hence, the main request is not allowable under Article 123(2) EPC.

4. *Auxiliary request: claim 1 - added subject-matter*

4.1 Added **feature (t)** does not address any of the deficiencies mentioned in points 3.1 to 3.3 above.

4.2 As a result, the auxiliary request is also not allowable under Article 123(2) EPC.

Order

For these reasons it is decided that:

1. The decision under appeal is set aside.

2. The patent is revoked.

The Registrar: The Chair:

B. Brückner K. Bengi-Akyürek

Decision electronically authenticated