Internal distribution code:

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

Datasheet for the decision of 9 December 2024

Case Number: T 2509/19 - 3.5.06

Application Number: 14739250.0

Publication Number: 2992475

IPC: G06F21/35, G06F21/43, H04L29/06

Language of the proceedings: EN

Title of invention:
Method for authentication, server, device and data carrier

Applicant:
Baseline Automatisering B.V.

Headword:
Two-factor authentication/BASELINE AUTOMATISERING

Relevant legal provisions:
EPC Art. 14(2), 56, 153(2), 153(5)
RPBA 2020 Art. 13(1), 13(2)

Keyword:
Inventive step - first auxiliary request (no)
Late-filed request - fourth auxiliary request (not admitted)

Decisions cited:
T 0700/05, T 1483/10, T 2692/18

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

Case Number: T 2509/19 - 3.5.06

D E C I S I O N
of Technical Board of Appeal 3.5.06
of 9 December 2024

Appellant: (Applicant)	Baseline Automatisering B.V. WG- Plein 568 1054 SJ Amsterdam (NL)
Representative:	Hoeben, Ferdinand Egon Allied Patents B.V. Postbus 1551 1200 BN Hilversum (NL)
Decision under appeal:	**Decision of the Examining Division of the European Patent Office posted on 14 March 2019 refusing European patent application No. 14739250.0 pursuant to Article 97(2) EPC**

Composition of the Board:

Chairman	M. Müller
Members:	R. de Man
	B. Müller

Summary of Facts and Submissions

I. The applicant appealed against the decision of the examining division refusing European patent application No. 14739250.0, which was filed in Dutch as international application PCT/NL2014/050278 and published in English as WO 2014/196852.

II. The examining division decided that the subject-matter of, in particular, the independent claims of the main request and of the auxiliary request lacked an inventive step over the following document:

D1: US 2008/0120711 A1, 22 May 2008.

III. With its statement of grounds of appeal, the appellant filed a marked-up copy of a set of claims of an amended sole main request and a marked-up copy of an amended description. It indicated that the amendments were intended to correct an error in the English translation of the application as filed.

IV. In a communication accompanying a summons to oral proceedings, the board expressed the preliminary opinion that the description and the amended claims of the main request violated Article 123(2) EPC and that the subject-matter of claim 1 of the main request lacked an inventive step over document D1.

V. With a letter dated 11 November 2024, the appellant retracted the amendments it had made to the description, maintained its main request and filed first and second auxiliary requests.

VI. During oral proceedings held on 9 December 2024, the appellant withdrew the main request and the second auxiliary request and later refiled the main request as the fourth auxiliary request (a third auxiliary request had been filed and withdrawn in the meantime). At the end of the oral proceedings, the chairman announced the board's decision.

VII. The appellant's final requests were that the decision under appeal be set aside and that a patent be granted on the basis of the claims according to the first or fourth auxiliary request filed with the letter dated 11 November 2024, the fourth auxiliary request having been filed as the main request.

VIII. Claim 1 of the first auxiliary request reads as follows:

"Method for authentication of a login of a client process into a server process by means of multiple communications comprising at least a primary authentication communication and a secondary authentication communication, wherein the method comprises steps for:

- the server process receiving from the client process an initiating communication (11) of the primary authentication communication (11,19),
- the server process sending an initiating communication (14) initiating the secondary authentication communication (14,16) between the server process and a client authentication process,
- the server process receiving primary authentication information comprising an authentication code or an authentication result by means of the primary authentication communication,

- the server process receiving from the client authentication process secondary authentication information (16) comprising an authentication code or an authentication result of the secondary authentication communication,

- the server process establishing (25,26) the authentication on the basis of the primary and secondary authentication information,

wherein the primary authentication communication (11,19) and the secondary authentication communication (14,16) are separate communications and/or wherein the server process can in itself establish a secondary authentication on the basis of the secondary authentication communication (14,16), and

- wherein the client authentication process is performed on a device that has been previously registered at the server by means of a prior verification comprising a step in which the user using an application comprising the client authentication process calls the server process being performed on the server and logs in by means of his/her login information known to the server."

IX. Claim 1 of the fourth auxiliary request differs from claim 1 of the first auxiliary request in that the text "a device that has been previously registered at the server" has been replaced with "a device that has been previously logged in at the server".

Reasons for the Decision

1. *The application*

1.1 The application relates to a two-factor authentication method by which a user can gain access to their account on a central server 3 using a client device 1 and a

previously registered mobile phone 2 (page 10, line 28, to page 11, line 5, and Figure 1 of the published application).

1.2 The user first authenticates themselves to the server 3 using client device 1 by means of a username and password (page 9, line 18, to page 10, line 8, and page 11, lines 15 to 21; Figure 1, messages 11 and 19, and Figure 2, steps 21 to 23; reference sign "12" on page 10, line 2, should apparently be read as "19").

The application refers to this phase as the "primary authentication".

1.3 When the primary authentication has been completed, the server 3 sends a challenge 14 to the mobile phone 2, and the mobile phone responds by means of a message 14 (page 10, lines 9 to 22, and page 11, lines 21 to 33; Figure 1 and Figure 2, steps 24 to 26).

Before sending the response message 14, the mobile phone 2 asks the user for confirmation (page 11, lines 26 to 28; page 12, lines 19 to 29).

The application refers to this phase as the "secondary authentication".

1.4 When the secondary authentication has been completed, the server sends a message 12 to the client device 1 to confirm that the user has successfully logged in (page 10, lines 28 to 31; page 11, line 33, to page 12, line 4; Figure 1 and Figure 2, steps 27 and 28).

1.5 The prior registration of the mobile device may involve the user first using the device to log on to the server (by means of "one factor authentication") and then

registering the device with the server (page 12, line 30, to page 13, line 20; Figure 5).

First auxiliary request

2. *Admittance into the appeal proceedings*

2.1 The first auxiliary request was filed in response to the board's communication and reverts the amendments to both the description and the claims made in the statement of grounds of appeal. Although the appellant had intended these amendments to correct mistakes in the English translation of the international application as filed, in the board's view the English translation contained no such mistake.

2.2 According to Article 14(2), second sentence, EPC, the translation of a European patent application into one of the official languages of the EPO may be brought into conformity with the application as filed throughout the proceedings before the EPO. In view of Article 153(2) and (5) EPC, which provides that Euro-PCT applications, i.e. international applications for which the EPO is a designated or elected Office, shall be treated as European patent applications, Article 14(2), second sentence, EPC applies also to the English translation of the present application (see decisions T 700/05, Reasons 4.1, and T 1483/10, Reasons 2.2).

2.3 Hence, since reverting the amendments made in the statement of grounds of appeal brings the English translation back into conformity with the application as filed, the board admits the first auxiliary request into the appeal proceedings.

3. *Inventive step*

3.1 Claim 1 of the first auxiliary request reflects the two-factor authentication method described in point 1. above:

- a primary authentication "communication" initiated by a "client process" involving the transmission of primary "authentication information" in the form of an "authentication code" or "authentication result" from the "client process" to a "server process";

- a secondary authentication "communication" initiated by the "server process" involving the transmission of secondary "authentication information" from a "client authentication process" running on a previously registered device to the "server process";

- the "server process" establishing that the "client process" has been authenticated on the basis of the primary and secondary authentication information;

- the previous registration at the server of the device for running the "client authentication process" involved "a prior verification comprising a step in which the user using an application comprising the client authentication process calls the server process being performed on the server and logs in by means of his/her login information known to the server".

3.2 Claim 1 further requires at least one of the features:

- the primary and secondary authentication "communications" are "separate communications"; and

- the "server process" can "in itself" establish a secondary authentication on the basis of the secondary authentication communication.

The board considers, and the appellant did not dispute, that these conditions are implied by the other features of the claim and therefore do not impose any further limitation on the claimed subject-matter.

3.3 The appellant argued that the invention did not merely register the device for running the "client authentication process" with the server but required the device to be "logged in with the server", which resulted in an ongoing session.

However, claim 1 of the first auxiliary request merely requires the device to have been previously registered with the server, where the registration process involved "a prior verification comprising a step in which the user using an application comprising the client authentication process calls the server process being performed on the server and logs in by means of his/her login information known to the server". Although the user has to log in to the server, this is needed only for the purpose of registering the device. The claim is silent on whether the user or the device remains "logged in", and this indeed plays no role for the proper functioning or security of the claimed two-factor authentication process.

3.4 Document D1 discloses the following multi-factor authentication technique, which is depicted in Figure 10:

- a first client computing device 910 initiates a first authentication process by transmitting a

first authentication request which includes a username and password combination to an authentication server 930 using a first communication channel (paragraphs [0079] and [0080]);

- the authentication server initiates a second authentication process by transmitting a second authentication request to a previously registered second client device 910 in the user's possession using a second communication channel different from the first communication channel (paragraphs [0079] and [0083]), and the second client device responds by transmitting an authentication code to the authentication server (paragraphs [0084] and [0085]);

- the authentication server establishes that the first client computing device has been authenticated on the basis of the authentication information (username/password and authentication code) received in the first and second authentication processes (paragraphs [0083] and [0090]);

- the previously registered device was registered with the authentication server "via a suitable user interface" (paragraphs [0083] and [0095]).

3.5 The subject-matter of claim 1 therefore differs from the disclosure of document D1 in that the user previously registered the device with the authentication server:

(a) by using an application comprising the "client authentication process", i.e. instructions

implementing the client side of the secondary authentication; and

(b) by logging in by means of login information known to the server.

3.6 The appellant argued that the formulation of distinguishing feature (a) did not sufficiently take into account that, in document D1, the secondary authentication process required the user to manually enter a string or handle a phone call, whereas the invention "merely opts to include a confirmation of will with the option to press a button".

However, claim 1 does not rule out that the "secondary authentication information comprising an authentication code or an authentication result" received by the server process from the client authentication process was entered or otherwise manually confirmed by the user. And this is in line with the appellant's own observation that the invention may "include a confirmation of will with the option to press a button" (as disclosed on page 11, lines 26 to 28, of the published application: "In step 25 is determined whether the user has given an acceptance, for instance within the valid time duration, by means of activating a button."). As an aside, the board notes that such a manual confirmation by the user, although not required by claim 1, appears to be an essential part of the two-factor authentication method of the present application (as well as that of document D1).

3.7 As for distinguishing feature (b), it is obvious that users attempting to register their device with the authentication server 930 of document D1 should be

authenticated first, for example by letting the user provide login information known to the server.

3.8 Distinguishing feature (a) requires the "client application process", which runs on a device corresponding to the "second client device" of document D1, to be implemented in an "application" which is also used to register the device with the server.

3.8.1 According to paragraph [0077] of document D1, a client computing device may be any computer-based communication device, including a personal computer, a PDA, a terminal device, a mobile telephone or a land-line telephone (paragraph [0077]). In an example given in paragraph [0083], the first client device used for the primary authentication is a desktop or laptop computer, and the second client device used for the secondary authentication is a telephone.

3.8.2 In the board's view, at the priority date of the application, i.e. on 29 April 2013, it was an obvious possibility to use instead, as the second client device, a smartphone device running an Android or iOS application implementing both the "client authentication process", i.e. the functionality necessary for carrying out the client-side part of the secondary authentication, and the client-side part of the registration process.

3.8.3 The appellant argued that the secondary authentication process of document D1 was implemented by means of the telephony network, the second client device being a regular telephone. The skilled person would have had no incentive to abandon this approach.

However, the skilled person needs no specific incentive to look for alternative implementations. Moreover, document D1 already discloses the use of alternative client computing devices such as PDAs.

3.8.4 The appellant further argued that the board's reasoning would imply that no computer program could ever be inventive.

This is not correct. The board's inventive-step reasoning starts from document D1, which discloses the functionality of the claimed "client authentication process" as part of a two-factor authentication method which is conceptually identical to the two-factor authentication method underlying the claimed invention. Therefore, the board's reasoning pertains specifically to the claimed invention and does not suggest any conclusion about the inventiveness of computer programs in general.

3.9 Hence, the subject-matter of claim 1 of the first auxiliary request lacks an inventive step over document D1 (Article 56 EPC).

Fourth auxiliary request

4. *Admittance into the appeal proceedings*

4.1 The fourth auxiliary request was filed during the oral proceedings before the board. It is identical to the main request withdrawn at the start of the oral proceedings.

As the fourth auxiliary request was filed when the main request was no longer part of the appellant's appeal case, its admittance is to be assessed under

Article 13(1) and (2) RPBA (see decision T 2692/18, Reasons 2).

4.2 Compared with the first auxiliary request, claim 1 of the fourth auxiliary request replaces the text "a device that has been previously registered at the server" in claim 1 with "a device that has been previously logged in at the server".

The appellant argued that the fourth auxiliary request should be admitted because this amendment overcame the board's objection of lack of inventive step by emphasising that the invention did not merely register the device for running the "client authentication process" with the server but required that device to be "logged in with the server", which resulted in an ongoing session (see also point 3.3 above).

4.3 The board notes that the wording "a device that has been previously logged in at the server" does not imply that the device remains logged in as part of an ongoing session, contrary to the appellant's argument.

Moreover, the amendment replacing "a device that has been previously registered at the server" with "a device that has been previously logged in at the server" broadens rather than narrows claim 1. Indeed, claim 1 of the first auxiliary request already requires the "device that has been previously registered at the server", which is the device on which the client authentication process is performed, to have been previously registered by means of "a prior verification comprising a step in which the user using an application comprising the client authentication process calls the server process being performed on the server and logs in by means of his/her login

information known to the server", i.e. the registration of the device involves a step in which the user uses the device to log in at the server.

Hence, at least *prima facie*, the amendment made in the fourth auxiliary request is unsuitable to overcome the board's inventive-step objection.

4.4 Since the fourth auxiliary request - being identical to the previously withdrawn main request - evidently could have been filed earlier, and since it is *prima facie* not allowable, the board does not admit it into the appeal proceedings (Article 13(1) and (2) RPBA).

5. Since the sole request admitted into the appeal proceedings is not allowable, the appeal is to be dismissed.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chairman:

A. Chavinier-Tomsic Martin Müller

Decision electronically authenticated