Internal distribution code:

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

Datasheet for the decision of 1 February 2021

Case Number: T 2018/14 - 3.5.06

Application Number: 10185106.1

Publication Number: 2315096

IPC: G06F1/00

Language of the proceedings: EN

Title of invention:
Flexible method of user authentication

Applicant:
ACTIVCARD IRELAND LIMITED

Headword:
User authentication/ACTIVCARD

Relevant legal provisions:
EPC Art. 84, 56

Keyword:
Claims - clarity (no)
Inventive step - (no)

Decisions cited:

Catchword:

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 2018/14 - 3.5.06

D E C I S I O N
of Technical Board of Appeal 3.5.06
of 1 February 2021

Appellant: (Applicant)	ACTIVCARD IRELAND LIMITED 30 Herbert Street Dublin 2 (IE)
Representative:	Ablett, Graham Keith Lewis Silkin LLP 5 Chancery Lane Clifford's Inn London EC4A 1BL (GB)
Decision under appeal:	**Decision of the Examining Division of the European Patent Office posted on 15 May 2014 refusing European patent application No. 10185106.1 pursuant to Article 97(2) EPC.**

Composition of the Board:

Chairman	M. Müller
Members:	T. Alecu
	B. Müller

Summary of Facts and Submissions

I. The appeal lies from the decision to refuse European patent application No. 10 185 106.1. The decision issued by reference to the communication dated 10 February 2014, which had been annexed to the summons to oral proceedings before the examining division and which found a lack of inventive step in respect of the subject-matter of claim 1 of the sole request over

D1: Yesberg J D *et al.*, "Quantitative authentication and vouching", Computers & Security, Elsevier Publishers, vol. 15, no. 7, January 1996, pages 633-645.

II. Notice of appeal was filed on 14 July 2014, the appeal fee being paid on the same day. A statement of grounds of appeal was received on 11 September 2014. The appellant requested that the decision under appeal be set aside and a patent be granted on the basis of the main (and sole) request as refused, consisting of claims 1-8 as filed on 7 March 2012, drawing sheets 1/6-6/6 and description pages 1-4 and 6-16 as originally filed, and description page 5 as filed on 31 August 2011.

III. In an annex to a summons to oral proceedings, the board informed the appellant of its preliminary opinion that the inventive step objection in view of D1 had to be confirmed, Article 56 EPC. A clarity objection was also raised, Article 84 EPC.

IV. In response to the summons, the appellant did not file either arguments or amendments. Instead, with letter of 5 January 2021, it informed the board that it would not

be attending the oral proceedings scheduled for 23 February 2021.

V. The oral proceedings were then cancelled as announced in the annex to the summons to oral proceedings.

VI. Claim 1 of the sole request reads as follows:

"A system for providing flexible user authorisation, the system comprising:

a plurality of clients, each having a security level associated therewith for a particular user, and each being capable of being accessed by the particular user upon the particular user having been granted a security level at least equal to the associated security level;

at least one data input device, each data input device being capable of providing user data relating to a user desiring access to a client,; and

a user authorisation module, the user authorisation module capable of performing a plurality of different user authorisation methods, each different user authorisation method for a particular user using a different set of user data from one or a combination of data input devices, wherein the user authorisation module determines a particular user authorisation method to be performed depending on a set of received user data for the particular user and performs the particular user authorisation method on the set of received user data provided by one or more data input devices by determining whether there is a match between the received user data and the stored reference user data within predetermined limits, and, if there is such a match, granting a security level for the particular user dependent on the particular user authorisation method used,

the system granting access for the particular user only to those clients that have an associated security level for the particular user at or below the security level granted to the particular user using the particular user authorisation method."

Reasons for the Decision

The invention

1. The application is generally concerned with access control to a computer system, especially to one comprising various resources (databases in particular) with different security requirements.

1.1 In the field, several methods are well-established, including user authentication with a password, with biometric information such as a fingerprint, a retinal scan or a voice scan, or based on smart cards or other security tokens.

1.2 The application addresses the problem that users may have reasons not to want or be able to use a particular authentication method, for instance because they have forgotten their smart card, because a fingerprint reader is not available at a particular workstation, or because the environment is too noisy to provide a voiceprint (see the description, page 11, lines 22-29). The invention is meant to provide the necessary flexibility without compromising security.

1.3 As a solution, the invention proposes to estimate the level of security that is achieved by using one or more individual user authorisation methods (see figure 3)

and to specify which security level is minimally required for a specific user to access a requested resource (see the table on page 12).

1.4 Users will identify themselves vis-à-vis the system by providing "user authorisation information" of their choice (see e.g. page 12, line 21, to page 13, line 22) and will be rated at the corresponding security level. Accordingly, information on the system will be "accessible" or "inaccessible" to the users (see page 13, lines 2-4, 6-8, 26-30).

The prior art

2. D1 proposes replacing the traditional binary authentication mechanism used in computer access control (according to which a user is or is not authenticated) by what is referred to as "quantitative authentication" (according to which degrees of authentication are considered; see abstract).

2.1 D1 discloses a variety of authentication mechanisms (see sections 2.4 and 4) with their respective advantages and disadvantages (see section 2.5) and that users accessing a system may have a different set of authentication mechanisms available in any given situation (because they may have forgotten their smart card, or because certain authentication devices are not provided at all machines for cost or other circumstances; see page 738, left column, paragraph 2, and page 640, left column, paragraphs 2 and 3, and right column, paragraphs 1 and 3).

2.2 A user to be authenticated will, according to D1, operate some of the available authentication devices (see section 3.2, (1)) which will issue corresponding

"certificates" (point (2)). An authentication server will associate an "authentication level" with the produced certificates based on an "authentication policy" (see points (3) and (4) and sections 3.4 and 3.5).

Clarity, Article 84 EPC, and claim construction

3. Claim 1 specifies that an authorisation method is "determined" depending on which "user data" the user has happened to provide.

3.1 The board considers that the method according to the invention does not require much "determination" at all.

3.2 In the board's understanding of the described invention, the user may present one or more different credentials, but each of them is simply authenticated with the appropriate method. That is, the methods for password or fingerprint authentication remain the same, irrespective of what credentials the user may also present. Also, user data can normally only be "provided" by the user if the corresponding "authorisation method" is "available": That is, a PIN can only be typed in as such when it is requested as such, and a fingerprint image can only be provided if the fingerprint reader is present and operational.

3.3 The system determines which credentials have been presented and authenticated and assigns a security level accordingly (see figure 3). The assignment of a security level however is not an authentication method.

3.4 In summary, the board considers that the mentioned language is potentially misleading and therefore renders claim 1 unclear, Article 84 EPC.

3.5 For the purpose of the following inventive step assessment, the board interprets the phrase "determines a particular user authorisation method to be performed depending on a set of received user data" as meaning not more than trying to authenticate the user based on the provided user data.

Inventive step

4. According to the decision under appeal (see point 2 of the communication of 10 February 2014), claim 1 differs from D1 in that

(a) each client is associated with a security level associated for a particular user, and
(b) the user authorisation module determines a particular user authorisation method to be performed depending on a set of received user data.

5. The examining division discussed the features separately. As regards feature (a), the examining division took the view that it was an administrative (i.e. non-technical) requirement that could not contribute to inventive step (see point 2.3 of the reasons). Feature (b) was considered to be a straightforward detail of implementing the use of various authentication devices (see point 2.4 of the reasons).

6. The board's position is as follows.

6.1 The appellant did not expressly challenge the finding that features (a) and (b) were the distinguishing features, and the board agrees with it. However, the appellant denied that features (a) and (b) could be considered separately, but provided no argumentation to

support this assertion (see the grounds of appeal, page 3, paragraph 2). The board considers the features separately, as it agrees with the opinion of the examining division on this point.

6.2 As regards feature (a), the board agrees with the examining division insofar as it is a matter of policy - and thus not technical by and of itself - to allow for security levels required at a client (i.e. for access of some service) to vary from user to user, i.e. that clients may associate "security levels" with "particular users".

6.3 The appellant contradicts this finding but its corresponding arguments seem not to go beyond the statement that implementing the policy in the system of D1 may require technical modifications (see grounds of appeal, page 3, paragraph 3, in particular lines 2-4). A statement with which the board agrees.

6.4 The implementation of such policies however is straightforward. It is already known from D1 that the certificates contain the claimant's name (see page 637, right column, paragraph 3). If the server's policy is to allow access to every user alike depending on its authentication level, the server can make do with storing the required security level. If the policy required that security level to vary with the user's identity, the server would have to store required security levels per user - as the appellant correctly points out (see grounds of appeal, page 3, paragraph 3, lines 6-8 from the bottom). This (slightly) increased complexity is, however, an obvious consequence of the required policy and would be easy for the skilled person to provide by way of modifying D1.

6.5 When discussing feature (a), the appellant submitted that D1 did not disclose the feature of *the system granting access for the particular user only to those clients that have an associated security level for the particular user at or below the security level granted to the particular user using the particular user authorisation method,* because D1 teaches no security levels per user.

6.6 The board notes that this feature is implicit in feature (a): Individual clients are associated with a security level associated for a particular user only so as to be able to grant access based on this information. So, if feature (a) were implemented by the skilled person in the context of D1, then (s)he would also implement the feature mentioned by the appellant.

6.7 As regards feature (b), the appellant relied on a literal interpretation of the claim, i.e. that there was a step of determining the authentication method depending on what "user data" was provided (see the grounds of appeal, page 3, last full sentence). As explained above (see point 3.4), the board considers the literal interpretation of this feature not to be the correct one, or at least not the only possible one. If feature (b) is construed as proposed above (see point 3.5), then this difference amounts to providing the user data to the server, instead of the certificates, and performing the respective authentication methods, i.e. matching the user data with the corresponding reference data, on the server. The board believes that the skilled person would consider this alternative implementation for various reasons, e.g. in order to increase the system security, as the reference user data would no longer be provided to the authentication devices, or in order to allow the

possibility of sensor-level data fusion for multibiometric authentication, which would for instance allow an assessment of biometrics orthogonality (see D1, last paragraph of section 3.4).

6.8 The board therefore affirms the examining division's conclusion that the subject-matter of claim 1 lacks inventive step over D1, Article 56 EPC.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chairman:

L. Stridde M. Müller

Decision electronically authenticated