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 9 May 2017

Case Number:	T 1135/11 - 3.5.06
Application Number:	01117879.5
Publication Number:	1176489
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 1973 Art. 56

Keyword:
Inventive step - (no)

Decisions cited:

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

Catchword:

Beschwerdekammern
Boards of Appeal
Chambres de recours

European Patent Office
D-80298 MUNICH
GERMANY
Tel. +49 (0) 89 2399-0
Fax +49 (0) 89 2399-4465

Case Number: T 1135/11 - 3.5.06

DECISION
of Technical Board of Appeal 3.5.06
of 9 May 2017

Appellant:m
(Applicant)

ACTIVCARD IRELAND LIMITED
30 Herbert Street
Dublin 2 (IE)

Representative:

Ablett, Graham Keith
Ablett & Stebbing
7-8 Market Place
London, W1W 8AG (GB)

Decision under appeal:

Decision of the Examining Division of the European Patent Office posted on 12 January 2011 refusing European patent application No. 01117879.5 pursuant to Article 97(2) EPC.

Composition of the Board:

Chairman W. Sekretaruk
Members: M. Müller
G. Zucka

Summary of Facts and Submissions

I. The appeal lies against the decision of the examining division, with reasons dispatched on 21 December 2010, to refuse European patent application No. 01 117 879. The decision cited in particular the documents

D1: JP 11 338826 A and
D4: EP 1 085 424

and argued that claim 1 of the main request did not comply with Article 123(2) EPC and that claim 1 of the auxiliary request lacked inventive step over D1, Article 56 EPC. The disclosure of D1 was discussed on the basis of its English family member D4.

II. A notice of appeal and a statement of grounds of appeal were filed and the appeal fee was paid on 11 March 2011. The appellant requested that the decision be set aside and that a patent be granted based on claims according to a main request or one of four auxiliary requests as filed with the grounds of appeal, in combination with the description and the drawings as originally filed.

III. In an annex to a summons to oral proceedings, the board informed the appellant of its preliminary opinion that claim 1 of all requests lacked novelty or inventive step over D4, Article 56 EPC 1973. Objections under Article 84 EPC 1973 were also raised.

IV. In response to the summons, with letter dated 6 April 2017, the appellant replaced all previous requests with newly filed main and auxiliary requests.

V. During the oral proceedings before the board, the appellant amended its main request twice and, once the board decided to admit the amended main request, withdrew its auxiliary request. The sole remaining request is based on claims 1-12 as filed during the oral proceedings at 11:00 hrs.

VI. Claim 1, the sole independent claim of this request, reads as follows:

"A method of accessing, through a workstation, a system having a plurality of resources with different associated security levels, wherein a plurality of user information entry devices are available at the workstation out of a plurality of supported user information entry devices supported by the system, the method comprising:

associating, at the system, different levels of security to different supported user information entry devices and different combinations of supported user information entry devices;

receiving, at the system, the user authorisation information from the workstation provided by the user using one or more of the available user information entry devices;

identifying, at the system, the user based on the received user authorisation information;

determining, at the system, which of the one or more user information entry devices were used to provide the received user authorisation information;

determining, at the system, the level of security of the identified user associated with the one or more user information entry devices used; and authorising user access to the plurality of resources within limits based upon the determined security level."

VII. At the end of the oral proceedings, the chairman announced the decision of the board.

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. Each of these methods has its own well-known advantages and disadvantages in terms of convenience, cost and security. For instance, a password is convenient to use but provides only low security. Retinal scanners and smartcards provide higher security but require dedicated hardware which may not be available at all access points. Passwords and smartcards may be forgotten or lost. Biometric data cannot be forgotten, but a fingerprint may be damaged by a cut and the user's voice may be distorted by a sore throat. Security may be increased by combining several authentication methods; say, a password with a fingerprint (see the description on page 4, lines 17-23; page 4, line 28, to page 5, line 7; page 7, lines 4-6; page 10, line 22, to page 11, line 12; page 13, lines 12-16).

1.2 The application addresses the problem that a user may have reasons not to want or be able to use a particular authentication method, for instance because he has forgotten his smartcard, 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 Any user will identify himself to the system by providing "user authorisation information" of his choice (see e.g. page 12, line 21, to page 13, line 22) and he will be rated at the corresponding security level. Accordingly, information on the system will be "accessible" or "inaccessible" to the user (see page 13, lines 2-4, 6-8, 26-30).

The prior art

2. The appellant has not challenged the assumption made by the examining division that for the purpose of examining the present application the disclosure of D1 is equivalent to that of D4. The board agrees and

refers to D4 on the understanding that its contents are prior art for the present application.

3. D4 discloses an architecture of a computer system (see figure 1) controlling access to a variety of services with different security requirements (see e.g. paragraphs 11 to 19 and 67).

3.1 In general terms, the system of D4 requires users requesting access to a service at a terminal (see e.g. paragraphs 2 and 131) to present an "authentication card" and to identify themselves, for instance by providing biometric data (see paragraph 28) as requested by the system (see paragraphs 41, 73 and 304). The biometric data is authenticated against reference data registered for that user (see e.g. paragraph 134) by an "authentication device" (see figures 2 and 3, esp. item 413, and paragraphs 139 to 146) or by the authentication card itself (see paragraph 29).

3.2 In the system of D4, the required level of security can be adapted by two primary measures. Firstly, the terminals are equipped with several different means for personal identification, which may be used separately or in combination (see paragraphs 111 to 112, 269, 131 to 136, and 324). And secondly, the registered biometric data is split and stored in different places. Some of that data is stored on the user's authentication card, the rest is spread over different "certification authorities" (see paragraph 173 and figure 1, items 7, 21, and 31). These authorities will only be involved if a higher level of security is required than that achievable by the biometric data on the card (see paragraph 27).

3.3 As a means of protection against misappropriation, D4 proposes that the user keep secret which credentials are stored on the card (and hence required for authentication) so that a thief will have to guess correctly in order to be able to use it (see paragraphs 111 to 113, but also 324).

Clarity

4. Amended claim 1 is clear enough to allow a substantive assessment of its subject-matter.

Claim construction

5. In D4, the kind of authentication required from the user is generally determined *after* the user has selected the service of interest and depending on that choice (*loc. cit.*). In the present invention, however, it appears to be intended that the user provides his choice of authentication data *before* accessing a certain resource - which is granted based on the security level associated with the authentication data provided.

5.1 The board however takes the view that the desired temporal order is not implicit in claim 1. More specifically, the claim language leaves open whether the claimed method is carried out before or after the user requests access to a given resource.

5.2 The crucial step of claim 1 in this regard is that of "authorising user access to the plurality of resources within limits based upon the determined security level". The appellant argued that this phrase had to be read as implying several subsequent accesses to resources which would be granted "within" predetermined "limits".

5.3 In the board's judgement, however, this interpretation is not mandatory. Rather, the cited language does not exclude the possibility that the desired resource access has been selected initially and is eventually "authorised" if the required level of security is below - i.e. "within limits based upon" - the determined security level. More than that: the board considers that the step of "authorising user access" in claim 1 does not imply any actual access to a resource and that the preamble of the claim according to which the claimed method is one "of accessing" does not imply a *step* of accessing. The board considers that the skilled reader would construe the claimed method as one of determining a security level for a particular user and storing that security level for later use in an undefined subsequent operation, possibly but not necessarily one of accessing a resource, but without including that operation.

Inventive step, Article 56 EPC 1973

6. D4 discloses methods of accessing, through terminals or "workstations", a system having at least one resource. Within D4, the board considers the most suitable starting point for assessing inventive step to be the embodiment according to which the card owner registers "authentication data selected from plural kinds of them" and keeps it secret in order to avoid misappropriation of the card (see paragraph 111).

6.1 A potential fraudster can only make guess wrongly if there are at least two "user entry devices" to choose from. Therefore, this embodiment implies that "a plurality of user information entry devices are available at the workstation out of a plurality of supported user information entry devices supported by the system".

6.2 The embodiment also implies that it must be determined "which of the one or more user entry devices were used to provide the received user authorisation information" and, moreover, that the user must be identified "based on the received user authorisation information".

7. The appellant argued that the following differences existed between D4 and the claimed invention.

(a) In D4, the claimed steps were not carried out on "the system having a plurality of resources" but rather locally (on the card or the authenticating device).

(b) D4 was less flexible than the claimed invention because in D4 it was obligatory for the user to carry an authentication card (which was not the case in the invention) and because the "user information entry devices" available at a terminal in D4 were predetermined and could not be changed without substantial effort (such as having to reissue many authentication cards).

7.1 The board disagrees that these differences exist.

7.2 *Re (a)* Firstly, the user identification according to D4 takes place, at least partially, on the remote certification authorities (see paragraph 27), i.e. not only locally. And secondly, the claim leaves undefined the architecture of the claimed "system having a plurality of resources". Therefore, if the access terminals 41 and the associated authentication devices 41 are identified with the claimed "workstations", the remaining part of the system depicted in figure 1 of D4 and any backend components needed for providing the requested service (see paragraph 131) constitute the claimed "system" accessed through a "workstation". Only in passing is it noted that, in the board's view, the skilled person does not generally need to exercise inventive skill in order to move a necessary step from a workstation to a separate "system" such as a server, since doing this has well-known advantages such as simplifying maintenance or reducing the workload on the workstations.

7.3 *Re (b)* While it is true that, in D4, the card is obligatory and the user information entry devices at any terminal are predetermined, the claimed invention does not exclude either. More specifically, the claimed method does not exclude the possibility that the user has to present an authentication card such as that of D4; and the method does not depend on the exact number or type of user information entry devices provided at the claimed workstation.

8. D4 is explicit about the fact that different services require different degrees of security and that certain types of biometric data may increase the level of security (see e.g. paragraphs 11 and 67). D4 also discloses that the system makes a decision based on which "level of authentication is required", namely whether or not to send the biometric data to the certification authority (see paragraph 27), but depending on the requested service. In the board's view this means that D4 discloses the relevant concepts. However, D4 does not disclose that the system represents and processes them explicitly. More specifically, D4 does not disclose that the security

level is determined separately from the authorisation decision made on it.

9. In summary, the subject-matter of claim 1 differs from the embodiment in D4 in that

(c) the accessed system has "a plurality of resources", especially ones "with different associated security levels",

(d) the "level of security associated with the [...] user information entry devices" is explicitly represented and determined.

9.1 *Re (c)* D4 discloses a large number of scenarios in which the authentication architecture can be used, including a variety of different services (and resources) and different security levels (see e.g. paragraphs 131, 199, and 241). The board considers it obvious that several such services can be provided by a single "system", be accessed through a single workstation and be associated with different security levels. This should, in the board's view, be self-evident for access to a medical database or to bank services via an automatic teller machine ATM, both mentioned in D4. For a concrete example, one might consider the case of an ATM offering several services (say, checking the account balance and retrieving money and charging a debit card) which make use of "different resources" (e.g. the debit card function depends only on the card, whereas the account balance must be retrieved from a database) and requiring different levels of security depending on the possible financial damage involved.

9.2 *Re (d)* As discussed above, the intended effect of associating a "security level" with a user depending on the user information entry device used is that the decision to grant or deny access to a resource can be made later. However, as also stated above, claim 1 does not imply the temporal order between determining the security level and accessing the resource, nor does it actually imply any step in which access to a resource is attempted and allowed or prohibited based on the "security level" with which the user is "authorised". The board considers that the explicit representation and processing of numbers representing "security levels" in claim 1 does not have or contribute to a technical effect. Even if the "security levels" could be used in a particular manner to achieve a technical effect, it could only be said that they had or contributed to that effect if that manner of use were explicitly claimed or otherwise a necessary consequence of the claim. This not being the case and according to established jurisprudence of the boards of appeal, it follows that feature (d) cannot contribute to inventive step.

10. The board therefore comes to the conclusion that claim 1 lacks inventive step over D4, Article 56 EPC 1973.

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

A. Wolinski W. Sekretaruk

Decision electronically authenticated