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 March 2016

Case Number: T 1590/13 - 3.5.06

Application Number: 06821334.7

Publication Number: 1952296

IPC: G06F21/00, G06F21/24

Language of the proceedings: EN

Title of invention:
SYSTEM FOR MANAGING ACCESS CONTROL

Applicant:
Koninklijke Philips N.V.

Headword:
Setting and adjusting access policies/PHILIPS

Relevant legal provisions:
EPC 1973 Art. 56
EPC R. 103(1)(a), 111(2)
RPBA Art. 11

Keyword:
Inventive step - both requests (no)

Decisions cited:

Catchword:

Europäisches Patentamt
European Patent Office
Office européen des brevets

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 1590/13 - 3.5.06

D E C I S I O N
of Technical Board of Appeal 3.5.06
of 9 March 2016

Appellant: (Applicant)	Koninklijke Philips N.V. High Tech Campus 5 5656 AE Eindhoven (NL)
Representative:	Uittenbogaard, Frank Philips Intellectual Property & Standards P.O. Box 220 5600 AE Eindhoven (NL)
Decision under appeal:	**Decision of the Examining Division of the European Patent Office posted on 27 February 2013 refusing European patent application No. 06821334.7 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 27 February 2013, to refuse European patent application No. 06 821 334.7 for lack of inventive step. Starting from a generic content distribution system, which the applicant agreed was known in the art, the examining division found that the invention lacked inventive step because it was the obvious implementation of a non-technical ("administrative") decision and, in addition, because the claimed matter was obvious in view of the following document:

D2: US 6 092 194 A.

II. A notice of appeal was filed on 18 April 2013, the appeal fee being paid on the same day. A statement of grounds of appeal was received on 4 July 2013. The appellant requested that the decision be set aside and that a patent be granted "on the basis of the enclosed claims 1-10, which correspond to the main request of the Decision" (see grounds of appeal, page 1, 2nd paragraph). Contrary to that statement, however, no claims were enclosed with the grounds of appeal, and the decision concerned claims 1-9 as filed during oral proceedings before the examining division (see annex to the minutes of the oral proceedings). The board therefore understands the appellant's request to be that a patent be granted based on *claims 1-9 as filed during oral proceedings before the examining division on 28 January 2013*, the other application documents being pages 1-3 and 3a as filed on 22 June 2012, and pages 4-19 and drawings pages 1-3 as originally filed. The appellant also requested the reimbursement of the appeal fee under

Rule 103(1)(a) EPC, because the decision was insufficiently reasoned (Rule 111(2) EPC).

III. In an annex to the summons to oral proceedings, the board informed the appellant of its preliminary opinion that the decision under appeal was not insufficiently reasoned and that the claimed invention lacked inventive step, Article 56 EPC 1973.

IV. In response, with letter dated 9 February 2016, the appellant filed amended claims 1-9 according to an auxiliary request. Furthermore, with letter of 7 March 2016, the appellant informed the board that it would not be represented at the oral proceedings but that it requested a decision on the file as it stands.

Claim 1 according to the main request reads as follows:

"Method for managing access control in a content distribution system, the system comprising
- at least one organization (32) for providing content data and related meta data,
- a rendering device (39) for rendering the content data and related meta data and executing the application, and
- at least one application for manipulating the content data and related meta data, which method comprises the steps of
- setting an access policy for the organization, called access policy of the organization, according to a predefined data access format, the access policy of the organization comprising access parameters for controlling access to resources of the rendering device and to content data and related meta data,
- providing at least one organization application (35) complying with the access policy of the organization,

- providing content data and related meta data complying with the access policy of the respective organization,
- executing the organization application while accessing the resources of the rendering device according to the access policy of the organization,
- setting by the user a user access policy that restricts access to the resources of the rendering device relative to the access policy of the organization, when executing the organization application, and
- adjusting the user access policy for the organization based on additional trust data for the organization for selectively allowing the organization application to access the resources according to the access policy of the organization."

Claim 1 according to the auxiliary request differs from claim 1 of the main request only in its last paragraph, which reads as follows:

"... - adjusting the user access policy by the rendering device (39) for the organization based on additional trust data for the organization received by the rendering device (39) from a remote database entity for selectively allowing the organization application to access the resources according to the access policy of the organization."

Both requests also contain an independent device claim, the wording of which corresponds closely to that of the respective independent method claim 1.

V. Oral proceedings were held as scheduled on 9 March 2016 in the absence of the appellant. At the end of the proceedings, the chairman announced the decision of the board.

Reasons for the Decision

The invention

1. The invention relates to a system in which "organizations" provide content and corresponding application software to an end user device which runs the application to "render" the content. For example, the content data might be video data in a proprietary format, the application might be required to access and display the data, and the device might be a suitable video player (see e.g. page 1, lines 19, to page 2, lines 12; page 3, lines 17-28; page 6, lines 2-14). Other types of content data and associated applications are possible (see, for instance, the references to "games" and "text reviews" on page 1, lines 21-22).

1.1 It is disclosed that "access policies" are provided in order to control applications when accessing, at the rendering device, the proprietary content and the resources of the rendering device (page 2, lines 9-12 and 15-18 and page 7, lines 18-21). These access policies may be enforced cryptographically at the rendering device (page 3, line 28).

1.2 It is observed that organizations providing software applications may be unknown or not trustworthy (page 3, lines 30-31; and page 12, lines 17-21), for instance because they may have gone out of business (page 4, lines 1-3) or were reported to "misbehave" (page 9, lines 27-29). It is also noted that an organization might be known and trusted by some users but not by others (page 4, lines 3-5), and that one user might find it acceptable if an organization accessed certain resources at the user's rendering device, whereas other

users might find that inacceptable (see page 3, lines 31-33).

1.3 The invention therefore proposes to enable individual end users to define "user access policies" which restrict which accesses the applications of an organizations are allowed to make (see e.g. page 9, lines 10-15, and page 12, lines 16-17). Such an access policy might, e.g., allow one user to disable all content of some organization to play, but it may also control the resource access more selectively (see page 9, line 22, to page 10, line 17). Moreover, the user access policy may depend on so-called "trust data for organizations", which may be held in a remote data base and which may contain "user feedback for specific organizations" (*loc. cit.*).

The prior art

2. In the decision, it is assumed that a method according to claim 1 except for the last two steps is "so well-known in the field of secure content distribution that written proof [is not] necessary". The existence of such method and corresponding system is reported to have been acknowledged by the appellant (see the decision, reasons 1.1 and 1.2) and this assumption is also not challenged in the grounds of appeal (see points 2.1 and 3.1).

3. D2 discloses a system for protecting Internet clients from "suspicious downloadables". D2 discloses a "security database" which includes security policies which may be specific for individual users or generic (default) (col. 4, lines 14-18). A requested download is carried out if the downloadable is determined to conform with the relevant policies as retrieved from the database (*loc. cit.* and col. 4, lines 62-65; fig. 3, no. 317). The policy management (fig. 2, no. 255; fig. 3;

col. 3, lines 62-63) is carried out at a server, i.e. the policies are not evaluated at the requesting client. D2 also discloses a "security policy editor" via which the user can effect modifications to the security policy (col. 7, lines 17-29).

The alleged substantial procedural violation, Article 11 RPBA

4. The appellant has argued that the examining division, in its argument based on D2, failed to explain "why the skilled person would [have] direct[ed] its attention to D2 and subsequently combine[d] the teaching of the closest prior art and D2". This being a crucial point in the problem-solution approach, the decision did thus not contain adequate reasoning as required by Rule 111(2) EPC (see grounds of appeal, page 6, point 4).

4.1 Firstly, the board notes that the decision contains two lines of reasoning to show lack of inventive step, only the second of which refers to D2. In its grounds of appeal, the appellant did not object to the first argument for insufficient reasoning. Hence, as the board noted in the annex to its summons, the insufficiency of reasoning alleged by the appellant did not affect the decision as a whole, and the board had to deal with the first objection independently of whether the second inventive step objection was actually found to be insufficiently reasoned.

4.2 Secondly, the examining division conceded that D2 and the invention were from slightly different contexts (see the minutes of the oral proceedings before the examining division, page 4, 2nd paragraph), but nonetheless considered D2 to establish that the skilled person was aware "that security policies can be amended". Moreover, it concluded that the skilled person would have adopted

the solution of D2 "for the same purpose" to solve the problem posed (see the decision, reasons 3.2, 3.4 and 3.6; and the minutes, page 4, 2nd paragraph). The board considered that this reasoning adequately addresses the concerns regarding D2 which the appellant raised during the oral proceedings (see the minutes). The board therefore disagrees with the appellant that the decision is insufficiently reasoned with regard to the second inventive step objection.

4.3 For these reasons, the board decided that it would be inappropriate to remit the case immediately to the first instance without assessing its merits (Article 11 RPBA), and issued summons to oral proceedings instead.

5. In its letter of reply of 9 February 2016, the appellant admitted that it had not addressed the first objection, but argued that the two objections overlapped and were thus "equally flawed", namely because the examining division had overlooked that the "problem of misbehaving organizations" required technical insight and addressing it was not a mere administrative choice (see that letter, pages 1-2, point 4). These arguments challenge the substantive correctness of the decision under appeal, but are unsuitable to establish that a substantial procedural violation occurred before the first instance. They could not, therefore, convince the board that the case should have immediately been remitted to the examining division under Article 11 RPBA.

Terminology

6. The claims do not define in detail the concept of an "access policy" or the nature of the "trust data". Likewise, they do not specify in detail, let alone in technical terms, how an access policy is represented, pro-

cessed and enforced, or how it is "adjusted" based on "trust data". The skilled person would therefore, in the board's view, take the terms "access policy" and "trust data" to define the relevant data only in terms of meaning, i.e. as defining which accesses are meant to be allowed or prohibited and under what conditions, and which "organizations" are meant to be trusted, under what conditions, and to what extent. The board also notes that the term "organization" has no specific meaning in technical terms and must be interpreted broadly. The claims also do not specify in any detail the rendering devices or the resources in question. The claimed rendering device could be a DVD player or a game console, but also, in principle, any personal computer. The resources in question could be any hardware component of the device, such as its hard disk, its Internet connection or its Webcam, and "restricting access" to these resources might mean blocking any access to the resources or imposing restrictions subject to certain constraints, e.g. time.

Inventive step

7. The appellant agrees with the decision under appeal that the invention according to claim 1 of the main request differs from the generic content distribution system (henceforth, "the known system") in the last six lines of claim 1, i.e.

1) setting by the user a user access policy that restricts access to the resources of the rendering device relative to the access policy of the organization, when executing the organization application, and

2) adjusting the user access policy for the organization based on additional trust data for the organization for selectively allowing the organization application to access the resources according to the access policy of the organization.

8. Claim 1 of the auxiliary request further differs from the known system by the facts that

3) the "adjusting" according to difference 2) is done "by the rendering device" and that

4) the additional trust data for the organization is "received by the rendering device [...] from a remote database entity".

9. The board considers that the inventive merit of the claimed invention turns on difference 1).

9.1 The appellant argues that feature 1) required "insight into the problem of misbehaving organizations and their effect on the [given] system", and that this was "technical insight" (see letter of 9 February 2016, page 1, last 8 lines) because it required an understanding that "misbehaving" organizations pose a security risk (see the grounds of appeal, points 3.1 and 3.2).

9.2 The board disagrees with this assumption. Rather, the board considers that any reservations, aversions or mistrust a user might have against an organization - be this a company, a political party, a governmental institution, or the operator of a certain website - is a non-technical matter.

9.3 The appellant challenges this argument, because it was not aware of "an instance where a complete organization

with multiple applications was distrusted before the priority date" and because there was no evidence on file "that users were distrusting each and every application issued by a particular organization" (see letter of 9 February 2016, page 2, paragraph 1).

9.4 The board takes the view that mistrust against an entire "organization" is a well-known phenomenon. For instance, some of the better-known software companies have attracted more reservations from within the user community the larger they have become. Political ideologies are known to focus on parties, countries, governmental organizations, particular newspapers or entire publishing houses. When parents decide that certain websites are unsuitable for the children below a certain age, this also represents mistrust against an "organization", broadly construed.

9.5 These observations do not, however, require proof, because the board considers reservations, aversions or mistrust against an entire organization to be non-technical anyway.

9.6 The board also considers that, from the reservations against an "organization", the desire naturally arises to block an application from that organization from running or from accessing certain resources of the rendering device, generally or only during predefined periods of time.

9.7 Therefore, the board considers that difference 1) addresses this desire and solves the problem of controlling the resource access of an application based on the users' "trust" vis-à-vis the organization providing that application.

9.8 From this perspective, the board finds it obvious to enable users to express their particular wishes themselves - i.e. to "set" their own "user access policy" in this respect - and to modify the rendering device to take into account these additional access policies.

10. As regards difference 2), the board agrees with the decision under appeal (see reasons 2.6) that "adjusting" an access policy is, in essence, a repetition or refinement of "setting" it.

10.1 The appellant stresses the difference between the two, noting that part 1 was clearly executed by the user, whereas part 2 did not state that the user was adjusting the user access policy (see letter of 9 February 2016, page 2, two last paragraphs). The board accepts this point.

10.2 The appellant further argues that part 2 stated the ad justment to be made "by the device" (*loc. cit.*).

11. As regards the main request, the board disputes this argument.

11.1 Claim 1 of the main request covers the situation that a user, having heard or read details about an "organization", decides to change its attitude towards that organization and modify its access policy, i.e. set a different one.

11.2 Therefore, the board concludes that claim 1 of the main request lacks inventive step as it is an obvious solution to a problem which can realistically be assumed to have arisen in the context of the known system, Article 56 EPC 1973.

12. As regards the auxiliary request, and in view of differences 3) and 4), the board accepts that claim 1 specifies the adjustment to be made by the rendering device.

12.1 However, even the auxiliary request leaves open how the rendering device is meant to adjust the user access policy "based on additional trust data". Specifically, it is not excluded that the rendering device acts in response to user input, for instance after having presented the "additional trust data" to the user for selection, addition, or confirmation. But even if one were to assume, for the sake of argument, that the "adjusting" was fully automatic and took place without any user intervention, the claimed adjusting step would not go beyond the straightforward automation of a "user access policy" based on unspecified "trust data" and according to certain predefined criteria, i.e. a number of non-technical decisions made by or on behalf of the user. The board considers it immaterial in this regard that the "setting" relates to "restrict[ing]", whereas the "adjusting" relates to "selectively allowing" access.

12.2 Therefore, part 2 differs from part 1 essentially in that the input based on which the access policy is defined ("set" or "adjusted") is not obtained from the user but from a "remote database entity".

12.3 In the board's view, these differences solve the additional problem of providing automatic support for the desired resource access control (see point 9.7 above).

12.4 That such automatic support is provided "by the rendering device" based on a "remote database entity" is considered obvious for the skilled person.

12.5 Therefore, claim 1 of the auxiliary request also lacks inventive step over the known system (Article 56 EPC 1973).

Inventive step in view of D2

13. In its letter of 9 February 2016 (page 3, lines 10-12; paragraph 2; paragraph 3, lines 4-6), the appellant argues that the skilled person trying to improve the control of the rendering device would have adopted the "readily available solution" according to D2 and that, D2 providing access control for individual applications but not for all applications "of" an organization, this would not have yielded the invention.

14. In this regard, the board only notes that inventive step of one solution cannot be established by showing that a different solution to the given problem exists and is obvious. Therefore, it is immaterial whether D2 might provide or suggest a different solution to the given problem. Thus, the board does not have to decide whether it agrees with the appellant that the claimed invention is not obvious over a solution based on D2.

Reimbursement of the appeal fee

15. Rule 103(1)(a) EPC states that the appeal fee may only be reimbursed in the event of interlocutory revision or where the board of appeal deems an appeal to be allowable. Therefore, the request for reimbursement of the appeal fee must be refused because the appeal is dismissed.

Order

For these reasons it is decided that:

1. The appeal is dismissed.
2. The request for reimbursement of the appeal fee is refused.

The Registrar: The Chairman:

B. Atienza Vivancos W. Sekretaruk

Decision electronically authenticated