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 4 March 2020

Case Number:	T 1746/17 - 3.5.07
Application Number:	04781683.0
Publication Number:	1665082
IPC:	G06F17/30, G06K9/00, H04L9/00
Language of the proceedings:	EN

Title of invention:
Methods and apparatus for content protection in a wireless network

Applicant:
QUALCOMM INCORPORATED

Headword:
Content protection/QUALCOMM

Relevant legal provisions:
EPC Art. 56, 84, 113(2)
EPC R. 99(2)

Keyword:
Basis of decision - interpretation of the appellant's requests
Admissibility of appeal - (yes)
Inventive step - main request and auxiliary request 2 (no)
Claims - clarity - auxiliary request 1 (no)

This datasheet is not part of the Decisior
It can be changed at any time and without notic

Decisions cited:

T 0255/05

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 1746/17 - 3.5.07

DECISION
of Technical Board of Appeal 3.5.07
of 4 March 2020

Appellant: QUALCOMM INCORPORATED
(Applicant)
5775 Morehouse Drive
San Diego, CA 92121 (US)

Representative: Dunlop, Hugh Christopher
Maucher Jenkins
26 Caxton Street
London SW1H 0RJ (GB)

Decision under appeal: **Decision of the Examining Division of the European Patent Office posted on 27 March 2017 refusing European patent application No. 04781683.0 pursuant to Article 97(2) EPC**

Composition of the Board:

Chairman R. Moufang
Members: R. de Man
C. Barel-Faucheux

Summary of Facts and Submissions

I. The applicant (appellant) appealed against the decision of the Examining Division refusing European patent application No. 04781683.0, published as international application WO 2005/026878.

II. The decision cited the following documents:

D1: "Methodology to Prevent Video and Software Piracy", IBM Technical Disclosure Bulletin, October 1993;
D2: EP 0 769 751 A1, published on 23 April 1997;
D3: US 2002/0125886 A1, published on 12 September 2002;
D4: EP 0 997 808 A2, published on 3 May 2000;
D5: WO 03/017053 A2, published on 27 February 2003.

The Examining Division decided that the subject-matter of all claims 1 to 8 of the main request and claim 1 of auxiliary requests 1 and 2 lacked inventive step over any of documents D1 to D5.

III. In its notice of appeal, the appellant requested that the decision under appeal "be set aside in its entirety". In its statement of grounds of appeal, the appellant requested that "the Decision under appeal either be set aside and a patent be granted on the basis of either the Main or the Auxiliary Request, or that the application be remitted to the Examining Division for further consideration".

IV. In a communication accompanying the summons to oral proceedings, the Board introduced the following document:

D7: L. Moureu, "Impact of location-based services on the mobility market", Alcatel Telecommunications Review, 2nd Quarter 2000, pp. 1-6.

It invited the appellant to clarify its requests and expressed doubts about the admissibility of the appeal. It also expressed the preliminary view that claim 1 of auxiliary requests 1 and 2 was not clear, and that the subject-matter of claim 1 of the main request and auxiliary requests 1 and 2 lacked inventive step over document D1.

V. In a letter dated 25 February 2020, the appellant informed the Board that it would not be attending the oral proceedings. It did not comment in substance on the Board's communication.

VI. Oral proceedings were held on 4 March 2020 in the appellant's absence. At the end of the oral proceedings, the chairman pronounced the Board's decision.

VII. Claim 1 of the main request reads as follows:

"A method (300) for operating a protection system (200) to protect an application (116, 220) from unauthorized operation, wherein the application (116, 220) will fail to operate on a device (102) that is outside a predetermined operating region, wherein the device (102) and the protection system (200) are coupled via a data network, the method comprising:

associating (306) a geographic identifier with the application (116, 220), wherein the geographic identifier identifies the predetermined operating region;

after said associating, downloading (308) the application (116, 220) and the geographic identifier to the device (102);

characterized by:

receiving (310) a request from the device (102) to execute the application on the device (102), wherein the request includes the geographic identifier;

determining (312) a device location;

comparing (314) the device location with the predetermined operating region identified by the geographic identifier;

sending (316) an authorization code to the device (102) allowing an execution of the application (116, 220) if the device (102) is within the predetermined operating region;

and

preventing (318) the application (116, 220) from executing when the device (102) is outside the predetermined operating region."

VIII. Claim 1 of auxiliary request 1 differs from claim 1 of the main request in that:

- the text "wherein associating includes using a device identifier, an application identifier and a region identifier to form a digital signature that represents the geographic identifier" has been added after "associating ... identifies the predetermined operating region";

- the text "characterized by:" has been deleted; and

- the text after "determining (312) a device location;" has been replaced with:

"generating another digital signature based on the device location;

determining whether there is a match (314) between the digital signature and the other digital signature;

sending (316) an authorization code to the device (102) allowing an execution of the application (116, 220) if there is a match."

IX. Claim 1 of auxiliary request 2 differs from claim 1 of the main request in that:

- the text "wherein the device is a mobile telephone," has been inserted after "on a device (102) that is outside a predetermined operating region";

- the text "characterized by:" has been deleted; and

- the text "by using a base station location, a system identifier, a network identifier or an area code" has been inserted after "determining (312) a device location".

X. The appellant's arguments, where relevant to this decision, are discussed in detail below.

Reasons for the Decision

1. *The appellant's requests*

1.1 In its statement of grounds of appeal, the appellant requested that the decision under appeal be set aside and that either a patent be granted on the basis of "either the Main or the Auxiliary Request" or the application be remitted to the Examining Division for further consideration.

Since the decision under appeal is based on a main request and two auxiliary requests (auxiliary requests 1 and 2), it is not immediately apparent how the appellant's reference to "the Auxiliary Request" is to be understood. Moreover, the appellant has chosen not to respond to the Board's invitation to clarify its requests.

1.2 A department of the EPO can decide upon a European patent application only in the text submitted to it, or agreed, by the applicant (Article 113(2) EPC). It is therefore the appellant's responsibility to define the text on the basis of which it requests that a patent be granted. In the case of auxiliary requests, this means that the appellant has to indicate the order in which its requests are to be examined and the content of each of these requests. If it fails to do so, there is no request that could be considered by the board (see decision T 255/05 of 18 October 2005, reasons 17 and 18).

1.3 However, in the present case the Board considers that it is sufficiently clear from the file what the appellant's requests are. Neither the notice of appeal nor the statement of grounds of appeal contains an indication that the appellant intended to modify its substantive requests, i.e. the main request and auxiliary requests 1 and 2 considered in the contested decision. In the Board's view, the most plausible explanation for the applicant's choice of wording that a patent be granted on "either the Main Request or the Auxiliary Request" is simply that the appellant overlooked the fact that its requests comprised a main request and not one but two auxiliary requests. In this respect, the Board notes that the statement of grounds of appeal makes no specific reference to the text of any of the requests but consistently refers only to "the invention".

1.4 Hence, the Board concludes that the appellant requests that the decision under appeal be set aside and that either (1) a patent be granted on the basis of the main request or, in the alternative, one of auxiliary requests 1 and 2 or (2) the application be remitted to the Examining Division for further prosecution.

2. *Admissibility of the appeal*

2.1 In its communication, the Board raised the question whether the statement of grounds of appeal indicated the reasons for setting aside the contested decision, as required by Rule 99(2) EPC. In particular, the Board questioned whether the statement of grounds of appeal contained arguments specifically addressing the decision's inventive-step reasoning.

2.2 The Examining Division essentially argued that all the technical features of the independent claims were known from each of documents D1 to D5. Any potential differences were therefore non-technical aspects, the implementation of which would have been obvious starting from any of documents D1 to D5.

2.3 The statement of grounds of appeal contains a number of arguments that, on careful consideration, do not address the decision's actual reasoning.

For example, the appellant argued that "technology, such as apps, smartphones, wireless communications etc" was not commonplace at the priority date in 2003; however, the reasons for the decision rely on prior-art documents D1 to D5 and not on a mere allegation of common general knowledge.

2.4 Likewise, the appellant's argument that the invention differs from the cited prior art in that "the security checking is done at a server remote from the device executing the software/application in question" does not explain why the appellant considers that the decision under appeal cannot be upheld. The reasons for the decision, for example with respect to document D1, do not assert that the prior art discloses that the check as to whether the device location is within the predetermined operating region is performed by an entity external to the device. The Examining Division apparently considered this aspect of the invention to be based on "non-technical, i.e. legal or administrative requirements" (see points 10.3, 11.2 and 16.2 of the reasons for the decision).

However, in its statement of grounds of appeal the appellant did give an argument rebutting this logical link in the Examining Division's chain of reasoning: it argued that carrying out the check at a remote server, and not locally, greatly enhanced security because it made the system less vulnerable to hacking or modification of the local device. In other words, the appellant argued that carrying out the check at a remote server had a technical effect and did not therefore merely follow from non-technical requirements.

2.5 Since the statement of grounds of appeal contains at least one argument addressing a crucial link in the decision's reasoning, and since this argument applies to the inventive-step reasoning with respect to each of documents D1 to D5, the statement of grounds of appeal does indeed comply with Rule 99(2) EPC.

2.6 As the appeal also complies with the remaining provisions referred to in Rule 101 EPC, it is admissible.

3. *The invention*

3.1 The invention relates to restricting the use of a downloadable software application to a predefined geographic region.

3.2 The content server from which the application is downloaded associates a geographic identifier with the application, identifying the geographic region to which use of the application is to be restricted. This identifier is downloaded to the downloading device together with the application.

3.3 When an application starts executing, it submits a request to the server/protection system that includes the geographic identifier. The server then determines the device's location and verifies whether that location is within the geographic region. If the verification is successful, the server sends an "authorization code" to the device, allowing the device to continue executing the application. Otherwise, the application is somehow prevented from continuing to execute.

3.4 Neither the description nor the claims contain any details about the "authorization code" provided to the application and how this code "allows" the application to execute on the device. The Board therefore considers that the term "authorization code" encompasses a simple code, such as a binary flag, which the application checks has been received before continuing its execution.

Main request

4. *Inventive step*

4.1 Document D1 discloses a method for preventing software piracy (page 1, lines 1, 2 and 19 to 21). To enforce "location-based group licensing", a geographic identifier of an operating region is associated with the software by hard-coding the coordinates of the target location into a customised copy of the software (page 1, lines 28 to 31). The software is then "sen[t] to that location" (page 1, lines 30 and 31). When the software starts executing, it calls on a GPS device to obtain the coordinates of the current location. If these coordinates do not match the hard-coded coordinates, the software "will not be started", i.e. it is prevented from executing (page 1, lines 31 to 34).

4.2 With respect to document D1, the appellant essentially argued that it disclosed neither the presence of a data network between the device executing the software and the system from which the software is distributed nor any receiving or transmitting means in the device. In particular, document D1 did not disclose "downloading the application and the geographic identifier to the device" because it referred, on page 1, lines 2 to 5, to "packaging individual copies of the software with hard copy documentation", which meant sending by post, and because the mention of "electronic distribution" in the same sentence was to be understood as referring to copying and circulation by users.

The Board understands the sentence on page 1, lines 3 to 5, as disclosing that copies of the software can be distributed both by post and electronically, the latter possibility referring to electronic transmission over a data network, i.e. "downloading". In the context of document D1 as a whole, the sentence on page 1, lines 30 and 31, therefore discloses that, at least as one possibility, the software including the hard-coded geographic identifier is sent from an implicit "content server" to the target location electronically over a data network, i.e. it is "downloaded" to the device.

4.3 The subject-matter of claim 1 differs from the disclosure of document D1 essentially in that the determination of whether the current device location is within the operating region is performed by the content server. More precisely, the content server:

- receives a request from the device to execute the application, wherein the request includes the geographic identifier;
- determines the device location;
- compares the device location with the predetermined operating region identified by the geographic identifier;
- sends an authorisation code to the device allowing an execution of the application if the device is within the predetermined operating region;
- prevents the application from executing when the device is outside the predetermined operating region.

4.4 In the Board's view, at the priority date of the application the skilled person would have been able, on the basis of his common general knowledge, to move operations carried out at a client device to a server device by means of a well-known request-response message exchange pattern. In other words, he *could* have modified the disclosure of document D1 to move the determination of the device location and the comparison of the device location with the geographic identifier from the device to the content server in the manner as claimed. The determination and the comparison would be carried out by the content server in response to a request by the client, and the content server would provide the outcome of the comparison, if positive, to the device in the form of an "authorization code" (e.g. as a binary flag; see point 3.4 above).

The question to be answered in order to assess inventive step is therefore whether the skilled person *would* have done so in expectation of the technical effect actually achieved by this modification (see Case Law of the Boards of Appeal, 9th edition, 2019, I.D.5). It is therefore necessary to examine what technical effect is actually achieved.

4.5 In its statement of grounds of appeal, the appellant argued that performing the security check at a remote server instead of the local device enhanced security because the local device was more vulnerable to hacking or modification.

However, if the local device can be hacked or modified, it is just as trivial a matter to bypass the security check at the remote server, for example by submitting a request that includes a geographic identifier corresponding to the actual device location to the server, or alternatively by executing the application even if no authorisation code is received (i.e. by not checking that the authorisation code has been received; see point 3.4 above). The Board therefore fails to see how the claimed remote security check improves security compared to the approach disclosed in document D1.

4.6 The appellant further argued - without further explanation - that carrying out the security check at a remote device allowed checking of the geographic location to be done "automatically without visibility to the user and while the user device is on the move from one location to another". However, the Board sees no reason why a local security check could not also be done automatically and while the device is on the move.

4.7 In the Board's view, performing the security check remotely at the content server merely has the expected advantages and disadvantages of moving an operation formerly performed at a client device to a server device. Such expected advantages and disadvantages cannot support an inventive step, since the skilled person *would* carry out a known modification in expectation of the technical effects expected from the modification.

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

Auxiliary request 1

5. *Clarity*

5.1 Claim 1 of auxiliary request 1 adds to claim 1 of the main request features specifying that the geographic identifier is a digital signature formed from a device identifier, an application identifier and a region identifier. When performing the security check, the content server/protection system generates "another digital signature based on the device location" and determines whether there is a match between the digital signature formed from the device, application and region identifiers and the ("another") digital signature formed from/generated on the basis of the device location.

5.2 The application does not explain how the digital signatures are formed or how two digital signatures are matched. Typically, a digital signature is generated by applying a cryptographically secure one-way function to one or more arguments representing the message to be signed. Two such signatures can be meaningfully "matched" only by verifying whether they are identical.

5.3 According to claim 1, the first of the two digital signatures to be matched is based on a device identifier, an application identifier and a region identifier, and the second is based on the device location. Since the claim lacks any further details in respect of the "forming"/"generating" and "matching" of the signatures (e.g. features specifying that the second digital signature is also based on the application identifier and the region identifier), it is not clear how determining a "match" between the two signatures could give meaningful information, such as an indication whether the device location is within the predetermined operating region.

5.4 Hence, claim 1 of auxiliary request 1 is not clear (Article 84 EPC).

Auxiliary request 2

6. *Inventive step*

6.1 Claim 1 of auxiliary request 2 adds to claim 1 of the main request features specifying that the device is a mobile telephone and that the device location is determined "by using a base station location, a system identifier, a network identifier or an area code".

6.2 As admitted in the present application's background art section (paragraphs [0002] to [0004]), mobile telephones to which applications could be downloaded were known at the priority date of the application.

It was further well known at that time that the location of a mobile telephone could be determined using a base station location, a network identifier or an area code (see document D7, page 4, right-hand column, lines 25 to 51; page 5, middle column, lines 19 to 34).

6.3 Hence, the features added to claim 1 do not add anything inventive. The subject-matter of claim 1 of auxiliary request 2 therefore lacks an inventive step (Article 56 EPC).

7. *Conclusion*

Since the Board has concluded that none of the requests on file complies with the EPC, there is no basis for allowing the appellant's request for remittal of the case to the Examining Division. The appeal is therefore to be dismissed.

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

S. Lichtenvort R. Moufang

Decision electronically authenticated