Internal distribution code:

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

Datasheet for the decision of 26 September 2019

Case Number: T 2164/13 - 3.5.06

Application Number: 07757500.9

Publication Number: 1987465

IPC: G06F21/00

Language of the proceedings: EN

Title of invention:
METHODS AND APPARATUS FOR PROTECTED DISTRIBUTION OF APPLICATIONS AND MEDIA CONTENT

Applicant:
QUALCOMM Incorporated

Headword:
Protected distribution/QUALCOMM

Relevant legal provisions:
EPC 1973 Art. 56

Keyword:
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 2164/13 - 3.5.06

D E C I S I O N
of Technical Board of Appeal 3.5.06
of 26 September 2019

Appellant: (Applicant)	QUALCOMM Incorporated Attn: International IP Administration 5775 Morehouse Drive San Diego, CA 92121 (US)
Representative:	Heselberger, Johannes Bardehle Pagenberg Partnerschaft mbB Patentanwälte, Rechtsanwälte Prinzregentenplatz 7 81675 München (DE)
Decision under appeal:	**Decision of the Examining Division of the European Patent Office posted on 13 May 2013 refusing European patent application No. 07757500.9 pursuant to Article 97(2) EPC.**

Composition of the Board:

Chairman	M. Müller
Members:	A. Teale
	B. Müller

Summary of Facts and Submissions

I. This is an appeal against the decision, dispatched with reasons on 13 May 2013, to refuse European patent application No. 07 757 500.9 on the basis that the subject-matter of claim 1 according to a main and two auxiliary requests did not involve an inventive step, Article 56 EPC, in view of the following document:

D1: US 6 832 318 B1.

II. A notice of appeal and the appeal fee were received on 22 July 2013, the appellant requesting that the decision be reversed and a patent granted. Oral proceedings were requested as an auxiliary request.

III. With a statement of grounds of appeal, received on 23 September 2013, the appellant filed amended claims according to auxiliary requests 1 to 4. The appellant requested that the decision be set aside and that a patent be granted on the basis of the main request on file or one of said four auxiliary requests.

IV. In an annex to a summons to oral proceedings the board set out its provisional opinion that it had doubts as to clarity and support, Article 84 EPC 1973, regarding claims 1 and 5 of all requests. The subject-matter of claim 1 of all requests, insofar as the clarity and support issues could be resolved by construction, seemed not to involve an inventive step, Article 56 EPC 1973, in view of D1. For the purposes of a decision in this case, there seemed to be no need to go further into the disclosure of any of the other documents cited in the decision or by the appellant.

V. In response to the board's summons, the appellant did not file any amendments or arguments. Instead, in a letter received on 1 July 2019, it requested a decision according to the state of the file and withdrew its request for oral proceedings. The board then cancelled the oral proceedings.

VI. The application is thus being considered in the following form:

Description (all requests):
pages 1 to 40, received on 9 September 2008.

Claims:
Main request: 1 to 14, received on 23 August 2012.
First to fourth auxiliary requests: 1 to 7, received on 23 September 2013.

Drawings (all requests):
Pages 1/12 to 12/12, received on 9 September 2008.

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

"A method for obtaining content in a protected environment, the method comprising: receiving a storage device comprising a storage device identifier and protected content; forwarding the storage device identifier to a network device; receiving at least a reference to a cryptographic mechanism from the network device based on an association with the storage device identifier; accessing at least a portion of the protected content with the cryptographic mechanism; characterized in that the method further comprises forwarding to the network device a request for access to at least one other portion of the protected content different from the portion accessed with the

cryptographic mechanism, the request comprising at least a computing device identifier and in particular the storage device identifier, the computing device identifier associated with a computing device operable to receive the storage device; receiving at least a reference to at least one other cryptographic mechanism from the network device based on an association with at least the computing device identifier and in particular the storage device identifier, the other cryptographic mechanism corresponding to at least the other portion of the protected content; and accessing at least the other portion of the protected content with the other cryptographic mechanism."

VIII. Claim 1 of the first auxiliary request essentially differs from that of the main request in the insertion of the following expression

"wherein said association does not involve a computing device identifier".

IX. Claim 1 of the second auxiliary request essentially differs from that of the first auxiliary request in the addition of the expressions "non-protected content" and "accessing the non-protected content, wherein the non-protected content includes limited-use content".

X. Claim 1 of the third auxiliary request essentially differs from that of the second auxiliary request in the insertion of the following expression

"wherein the step of accessing the non-protected content further defines the limited-use content as being limited-use content based on a computing device that receives the storage device".

XI. Claim 1 of the fourth auxiliary request essentially differs from that of the third auxiliary request in the insertion of the following expression

"wherein the limited-use limits the use to a predetermined finite number of uses or plays, to a predetermined limited time period in which the non-protected content may be available, to a predetermined set of functionality less than the full functionality of the protected content, or to an accessibility to a predetermined limited portion of the full amount of content".

Reasons for the Decision

1. The admissibility of the appeal

In view of the facts set out at points I to III above, the appeal fulfills the admissibility requirements under the EPC and is consequently admissible.

2. A summary of the invention

2.1 The application relates to distributing media content and applications on a removeable data storage device, such as a CD or flash card, in a way which respects the associated intellectual property rights and which is seamless (see [75]) and places a minimal burden on the user of the storage device, see paragraphs [1-4]. The data storage device is used with a computing device (see figure 2; 20) having a computing device identifier (29). The computing device can be a mobile device, such as a wireless communication device (see figure 1; 20A), or it can be a fixed desktop computer (20D). In particular, the invention seeks to provide a data

storage device for storing a large volume of content and/or applications, only portions of which require protection by encryption using a content key; see paragraphs [7, 29].

2.2 As shown in figure 1, the data storage device (10) comprises a "data storage identifier" (16) and several items of protected content (14), each having a content identifier. The data storage device may also store non-protected (freely accessible) content; see figure 2; 15 and [34-36]. The user's computing device (20) sends a data storage device identifier and a content identifier (18A, 18B) for each item of content (14A, 14B) to be accessed to a network device (see figures 1 and 2; 40) which, if the protected content is recognised, responds with a different content key (42) (termed "references to cryptographic mechanisms" in the claims) for each item which are then used to access the items of content; see paragraphs [32, 37].

2.3 The first auxiliary request is directed to the embodiments in which the content key is not associated with a computing device identifier; see original claim 1 and paragraphs [27-37]. The second and fourth auxiliary requests are directed to embodiments in which the storage device also contains non-protected content including limited-use content; see original claims 13 and 23. The third auxiliary request focuses on the embodiments in which the limits placed on the use of non-protected content depend on the computing device; see page 10, lines 1 to 5. In the fourth auxiliary request the limits on content use are set out, namely a finite number of uses, a limited time period of use and less than full content functionality; see page 9, line 29, to page 10, line 1.

3. Clarity, Article 84 EPC 1973

There is no need to determine whether the doubts raised in the annex to the summons to oral proceedings amount to a violation of Article 84 EPC 1973. This is because the board finds that the claims of all requests, understood in the light of the application as a whole, are sufficiently clear for the assessment of inventive step and, as will be shown, this assessment alone is decisive for all requests.

4. Document D1

4.1 The appealed decision starts from D1. As illustrated in figure 1 (see also column 10, lines 10 to 64), D1 relates to distributing data, for instance books, audio or video recordings, in encrypted form on distribution CDs (120)(hereinafter "CDs") to users equipped with an information access system (130, 140, 150) for reading the CD. In addition to encrypted data, each CD also contains a unique disc identification including a disc ID number; see figure 2; 200, 250 and column 11, lines 37 to 43. A central access control system (100) comprises a database containing, for each disk, its identification information, a "remote location access rights list" (ARL) and the intended recipient remote location; see column 9, lines 9 to 18. Each "remote location" is equipped with an information access system, including a unique remote location identification number, a CD reader and a decryption system, the information access system being linked via a bilateral communication link (132, 142, 152) to the central access control system.

4.2 A user wishing to access information on the CD logs onto the information access system (130, 140, 150), the

information access system reads the disc information and sends its unique remote location identification number and the disc identification information as an access request (see figure 3, step 10 and column 12, lines 29 to 33) to the central access control system (100); see column 9, lines 24 to 37. If the request is verified by the central access control system (100), taking into account the access rights list (ARL), then the requesting information access system is sent a unique decryption key to decrypt and access its CD; see column 12, lines 51 to 61.

4.3 The unique remote location identification number of each information access system can be a public encryption key, the central access control system also using that public key to encrypt the distribution CD's decryption key; see column 9, lines 38 to 43, and figure 3B, steps S13 to S15.

4.4 Hence in D1 encrypted content is distributed by CD, whilst the key required to decrypt and access the content on a particular CD is distributed via a computer network. The decryption keys are used to decrypt the whole CD (see figure 3B, step S17), there being no suggestion that different keys are required to decrypt different portions of the CD or that only a portion of the CD is encrypted.

4.5 The board regards the distribution CD (120) in D1 as a "storage device" in the claims. The disc identity information (200) is a "storage device identifier" in the claims. The central access control system (100) forms a "network device" in the claims. Hence claim 1 of the main request is correctly delimited against D1. Since the decryption key in D1 is used to decrypt and access the whole distribution CD, there is no

disclosure of a request to the central access control system for a decryption key to access one other portion of the CD.

5. The appellant's substantive requests

5.1 The main request

5.1.1 The claims of the main request are the same as those in the decision, according to which the subject-matter of claim 1 differed from the disclosure of D1 in that the protected content stored on the CD included several "portions", each one needing a different "reference to a cryptographic mechanism". This difference addressed the problem of refining the granularity of access control to the content. This problem was common in computer security, the balance between protecting content and the effort required being well known. The use of different keys to protect different parts of the content, set out in claim 1, was known as an alternative to using a single key for the complete data carrier; see, for example, D4. D4 disclosed the use of "title keys", as explained in page 8, section "3.2.3.1 Encrypted Title Key and CCI (Copy control Information)". A different title key was used per title. The selection of a known alternative, producing no surprising effect, did not involve an inventive step. Moreover the use of a key per part of content derived from an administrative rule rather than technical considerations. Hence the difference did not solve a technical problem and thus could not contribute to inventive step.

5.1.2 It is common ground between the appellant and the decision, and the board agrees, that D1 does not disclose

"receiving at least a reference to at least one other cryptographic mechanism from the network device based on an association with at least the computing device identifier and in particular the storage device identifier, the other cryptographic mechanism corresponding to at least the other portion of the protected content, and accessing at least the other portion of the protected content with the other cryptographic mechanism."

5.1.3 The appellant has also stated that the "remote location identification" known from D1 cannot be understood as a "computing device identifier", set out in the claims.

5.1.4 According to the appellant, the decision alleged that "the use of different content keys to protect different parts of the content is known as an alternative solution to the use of a single key for the complete carrier", but did not show that this was known at the priority date. The decision also did not explain why using several keys was an "alternative" to using a single key, since the use of several keys was at least more complex.

5.1.5 Regarding the problem solved by the characterising features over D1, the board finds that the objective technical problem cannot be fairly framed as refining the granularity of access control to the content, since this problem points to the solution. Point 1.9 (page 6) of the decision states that the use of a key per part of content derives from an administrative rule. The board takes the view that the objective technical problem starting from D1 can indeed be regarded as implementing an aim to be achieved in a non-technical field, namely to enforce different licence conditions

for the different works on a distribution CD in D1. This aim is reasonable, given the fact that D1 mentions CDs being used to distribute audio and video recordings, software books and multimedia works; see column 1, lines 50 to 52.

5.1.6 The skilled person, starting from D1 and implementing the method known from D1 in a way which achieves the above non-technical aim, would seek to provide independent access control to the various works on the distribution CD. The person skilled in the art of media distribution would have refined the granularity of CD access control known from D1 by requiring that the user request a different decryption key for each work on the CD, i.e. different portions of the CD, as a matter of usual design.

5.1.7 Hence the subject-matter of claim 1 does not involve an inventive step, Article 56 EPC 1973.

5.2 The first auxiliary request

5.2.1 Compared to claim 1 of the main request, claim 1 of this request additionally sets out the feature (based on paragraph [60], first sentence) that the association (between the reference to the cryptographic mechanism and the storage device identifier) does not involve a computing device identifier.

5.2.2 According to the appellant, this amendment addresses the objection in the decision that merely setting out the storage device identifier does not exclude the provision of further information.

5.2.3 The method known from D1 also does not involve a "computing device identifier" in the sense of the

application, since in D1 the "remote location identifier" (which is not defined in more detail) is understood as indicating a location rather than a device, namely the information access system. The appellant argues along the same lines in points 3 to 6 of the grounds of appeal. Even if one were to consider the remote location identifier in D1 as *de facto* a computing device identifier, not taking the computing device identifier into account would have been usual in implementing licensing conditions which are device-independent.

5.2.4 Hence the additional feature is unable to lend inventive step to claim 1, Article 56 EPC 1973.

5.3 The second auxiliary request

5.3.1 The claims of this request are similar to those of the first auxiliary request in the decision. According to the decision, claim 1 set out the additional features (based on original claims 11 and 13) that the storage device also contained non-protected content and the method also comprised accessing the non-protected content that included limited-use content. The added features were a juxtaposition over the existing features, since they did not address the problem of providing a more flexible and secure mechanism for obtaining content, as stated by the applicant. Neither did they address the problem of refining the granularity of access control. The added features appeared to be based on commercial or contractual restrictions and were thus unable to contribute to inventive step. At the priority date DVDs were known which presented different previews based on the selected language.

5.3.2 The appellant has argued that the added features are not known from any document on file and further reduce the time and power required to encrypt and decrypt content. There was also a synergistic effect because the computing device identifier could be used to define the limited-use content. The decision also failed to cite any evidence of a prior art disclosure of DVDs presenting different previews depending on a language selection.

5.3.3 The board regards providing a work on the distribution CD which is not encrypted as an extreme example of licensing conditions, an option which the skilled person achieving the above non-technical aim, would have realised as a matter of usual practice. The claim does not set out how the use of "limited-use content" is enforced and hence covers non-technical methods of enforcement, for instance threats of legal consequences, should a work be used contrary to its license conditions. Hence the references to "limited-use" content are unable to contribute to inventive step.

5.3.4 Thus the additional features are unable to lend inventive step, Article 56 EPC 1973, to claim 1.

5.4 The third auxiliary request

5.4.1 The claims of this request are similar to those of the second auxiliary request in the decision, according to which claim 1 was now further limited by the feature (based on original claim 14) that the limited-use content of the non-protected content was limited based on the computing device that received it. The additional feature was based on commercial considerations regarding limiting a player's access to

non-protected content. The limitation was not expressed as technical features but rather by setting out the rule to be implemented by the skilled person. The claim also did not set out the computing device being linked to the non-protected content, so the addition did not improve security. As no technical problem was solved, the additional feature could not contribute to inventive step.

5.4.2 Regarding the third (and fourth) auxiliary request, the appellant has argued that the added feature further refined the avoidance of encrypting and decrypting content, saving time and energy and thus going beyond the implementation of an administrative rule.

5.4.3 The board agrees with the examining division. The claim does not set out how the use of "limited-use content" is enforced and hence covers non-technical methods of enforcement, for instance threats of legal consequences, should a work be used contrary to its license conditions. Hence the references to "limited-use" content are unable to contribute to inventive step.

5.4.4 Hence the board finds that the additional features are unable to lend inventive step, Article 56 EPC 1973, to claim 1.

5.5 The fourth auxiliary request

5.5.1 Compared to claim 1 of the previous request, claim 1 of this request sets out the following additional features (based on paragraph [36])

"wherein the limited-use limits the use to a predetermined finite number of uses or plays, to a

predetermined limited time period in which the non-protected content may be available, to a predetermined set of functionality less than the full functionality of the protected content, or to an accessibility to a predetermined limited portion of the full amount of content".

5.5.2 The above passage sets out a list of alternatives ("or") for the limited uses. Regarding the first two limitations, namely of uses/plays and time period, the claim does not set out how the use of "limited-use content" is enforced and hence covers non-technical methods of enforcement, for instance threats of legal consequences, should a work be used contrary to its license conditions.

5.5.3 Hence the references to "limited-use" content are unable to contribute to inventive step and the board finds that the additional features are unable to lend inventive step, Article 56 EPC 1973, to claim 1.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chairman:

L. Stridde M. Müller

Decision electronically authenticated