Internal distribution code:

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

Datasheet for the decision of 12 March 2019

Case Number: T 1473/17 - 3.5.06

Application Number: 11816757.6

Publication Number: 2593859

IPC: G06F7/04, H04L29/06, H04N21/258, H04N21/472, H04N21/658

Language of the proceedings: EN

Title of invention:

APPARATUS AND METHODS FOR CONTENT MANAGEMENT AND ACCOUNT LINKING ACROSS MULTIPLE CONTENT DELIVERY NETWORKS

Applicant:

Time Warner Cable Enterprises LLC

Headword:

Account linking across networks/TIME WARNER

Relevant legal provisions:

EPC Art. 84, 123(2)
EPC R. 111(2)
RPBA Art. 11

Keyword:
Decision insufficiently reasoned (yes)
Fundamental deficiency (yes)
Special reasons for not remitting the case (yes)
Claims - clarity (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 1473/17 - 3.5.06

D E C I S I O N
of Technical Board of Appeal 3.5.06
of 12 March 2019

Appellant: (Applicant)	Time Warner Cable Enterprises LLC 60 Columbus Circle New York, NY 10023 (US)
Representative:	Dolleymores 9 Rickmansworth Road Watford, Hertfordshire WD18 0JU (GB)
Decision under appeal:	**Decision of the Examining Division of the European Patent Office posted on 6 February 2017 refusing European patent application No. 11816757.6 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 is against the decision of the examining division, with reasons dispatched on 6 February 2017, to refuse European patent application No. 11 816 757 for lack of novelty and clarity (main request) and lack of clarity (auxiliary request 3). Auxiliary requests 1 and 2 were not admitted pursuant to Rule 137(3) because they did not, "prima facie", meet the requirements of Article 123(2) EPC.

II. Appeal was filed on 13 April 2017, the appeal fee being paid on the same day. A statement of grounds of appeal was received on 15 June 2017. The appellant requested that the decision be set aside and that a patent be granted on the basis of claims 1-15, filed with the grounds of appeal, of a main or one of three auxiliary requests. Auxiliary requests 1 and 2 at that point were, up to marginal modifications, identical with auxiliary requests 1 and 2 as subject to the refusal.

III. In an annex to a summons to oral proceedings, the board informed the appellant of its preliminary opinion that the subject-matter of the claims on file lacked inventive step, Article 56 EPC, and clarity, Article 84 EPC.

IV. In response to the summons, with letter dated 17 January 2019, the appellant filed amended claims 1-15 according to a main and a sole (first) auxiliary request. Auxiliary requests 2 and 3 were not maintained.

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

"A method (300) for providing protected content via a first network (202) operated and controlled by a

service provider, to an authorized user (106, 107) of a second network (201) separate to the first network and operated and controlled by a network operator separate to the service provider, the two networks being connected by a network external to both the first and second networks, said method comprising:

receiving at an entity (204) of said second network a request for said protected content, said request comprising at least information identifying a requesting user and information identifying requested content;

determining at the second network, based at least in part on said information identifying said requesting user, an identity of said requesting user as said authorized user of said second network;

generating at the second network a unique identifier for said authorized user; and

transmitting a response to said request to an entity of said first network, said response comprising said unique identifier;

the method being **characterized in** further comprising positioning content protection data at said entity of said first network, said positioning enabling said operator of said second network to maintain integrity of said protected content outside of said second network and within said first network in accordance with a policy specified by an operator of said second network using said positioned content protection data, said positioned content protection data being specific to said requesting user;

wherein, said transmission of said response is configured to cause said entity of said first network to apply said content protection data to the requested protected content and to deliver said protected content to a device of said authorized user; and

wherein said unique identifier is stored at said entity of said first network, the method further comprising:

receiving at said entity of said first network a subsequent request from said requesting user, said subsequent request comprising a request for protected content different to that previously requested;

using said stored unique identifier to identify the previously positioned content protection data specific to said requesting user; and

applying said previously positioned content protection data to the subsequently requested protected content prior to delivery to a device of said requesting user."

Claim 1 of the auxiliary request differs from claim 1 of the main request in the characterizing portion which reads as follows:

"... the method being **characterized in** said protected content being protected in accordance with a policy specified by an operator of said second network, by encrypting said content using an encryption mechanism comprising a public/private key assigned to said authorized user by an operator of said first network, which public/private key is specific to said authorized user, the method further comprising positioning cryptographic data at said entity of said first network, said positioning enabling said operator of said second network to maintain integrity of said protected content outside of said second network and within said first network;

wherein said transmission of said response is configured to cause said entity of said first network to apply said content protection data to the requested protected content and to deliver said protected content

to a device of said authorized user, said delivered protected content comprising content at least partly encapsulated using an Internet Protocol (IP);

wherein said unique identifier is stored at said entity of said first network, the method further comprising:

receiving at said entity of said first network a subsequent request from said requesting user, said subsequent request comprising a request for protected content different to that previously requested;

using said stored unique identifier to identify the previously positioned cryptographic data specific to said requesting user; and

encrypting the subsequently requested protected content using said previously positioned cryptographic data prior to delivery to a device of said requesting user."

VI. In a telephone conversation on 24 January 2019, the board informed the appellant that the date for oral proceedings was maintained because at least the two "separate networks" would still have to be discussed under the requirements of clarity and inventive step.

VII. With letter dated 22 February 2019, the appellant informed the board that it would not be attending the scheduled oral proceedings.

VIII. Oral proceedings were then cancelled.

Reasons for the Decision

The invention

1. The application relates to content delivery across several networks (see the description as published, page 1, last paragraph).

1.1 It is described that, while such networks have proliferated (see page 2), "current systems offer no mechanism for a managed network operator (e.g., MSO)" (see also page 8, lines 20-22; "MSO" = "multiple systems operator", see page 8, lines 20-22) "to partner with service providers" so that verified users of the MSO network can access content "via the Internet or another such external network or internetwork via partnered service provider websites or similar portals" (see page 2, lines 24-29). As a solution to this problem, the invention can be paraphrased as proposing that the MSO network offer customer authentication *as a service* to the partnered service providers (see page 3, lines 9-14, and page 9, lines 24-26 *et seq.*; see also figure 2).

1.2 Responsible at the MSO network for the authentication service are an "entitlement server" and an "identity provider" (see e.g. page 17, last paragraph; page 18, paragraph 3; figure 2, nos. 208 and 210).

1.3 Different embodiments of the general idea are disclosed: For example, the user may login to a "third" service provider's website, which will identify the user as usual and forward any request to access protected content to the MSO network (see page 10, lines 11-15; figure 2b). The user may also log directly

into the MSO network (page 10, lines 4-10; figure 2a). Furthermore, "MSO-specific information regarding" the user's "identity" (such as a globally unique identifier, a GUID) may be "stored at the service provider site", for instance so as to speed up subsequent, further requests for content (see page 10, lines 16-25; page 17, lines 2-8; page 18, lines 20-30; page 23, lines 12-17; page 24, lines 15-19).

Article 123(2) EPC, Rule 111(2) EPC, Article 11 RPBA

2. The examining division stated in its decision (see points 2 and 3 of the reasons) that claim 1 of auxiliary requests 1 and 2 did not, "prima facie", meet the requirements of Article 123(2) because it could not identify an "appropriate basis" for the following two passages of respective claim 1:

"wherein said unique identifier is stored at said entity of said first network and is used in applying digital rights management or other forms of content protection in response to a subsequent request from the authorized user for different protected content, prior to delivery of that content, which digital rights management or other forms of content protection are specific to said requesting user."

and

"wherein said unique identifier is stored at said entity of said first network and is used in encrypting said content in response to a subsequent request from the authorized user for different protected content, prior to delivery of that content, which encryption is specific to said requesting user."

2.1 During the oral proceedings before the examining division, the appellant had referred to the paragraph bridging pages 40 and 41 and the last paragraph of page 10 as basis for these amendments.

2.2 The examining division did not, in the decision, explain why it did not consider the references given by the appellant to be "appropriate basis" for the purposes of Article 123(2) EPC. In fact, the decision does not mention the basis indicated by the appellant, let alone discuss it in any detail. This is insufficient reasoning even for a mere "prima facie" assessment. The board therefore concludes, in this regard, the decision not to be reasoned within the meaning of Rule 111(2) EPC and the first instance proceedings to be fundamentally deficient in the sense of Article 11 RPBA.

2.3 However, the board took the facts that this deficiency does not apply to the decision about the main request and that all requests filed on appeal shared several clarity problems (see the annex to the board's summons) to constitute special reasons under Article 11 RPBA for not remitting the case without consideration of its merits.

2.4 Whether the objection is correct in substance need not be decided, however, *inter alia* because the two pertinent features are not contained in claim 1 according to the two present requests.

Clarity, Article 84 EPC, and claim construction

3. The board considers that the independent claims of both requests are unclear, for the following reasons.

4. According to its preamble, claim 1 of both requests relates to providing content "via a first network [...] to [a] user of a second network", the networks being "connected by a [third] network external to both the first and the second networks".

4.1 It is not specified in what way the first and second networks are "separate". However, in the board's judgment the skilled person would understand, also in view of the "connect[ing]" third network, that the "entities" constituting the networks are disjoint, i.e. that no "entity" or "device" can belong to both networks.

4.2 In its remainder, however, claim 1 focuses on merely a few entities or devices of the two networks.

4.3 A user's request is received at an "entity" of the second network, a corresponding "response" is generated and transmitted to an "entity" of the first network and, eventually, content is delivered to "a device of [the] requesting user". The board takes it that the skilled person would understand the device as part (i.e. an "entity") of the second network or, at least, that delivery to the user's device passes through an "entity" of that second network. This leaves open whether the requesting entity is the same as the device to which the content is delivered.

5. It is unclear in what way the first and second networks limit the claimed subject-matter.

5.1 Some of the method steps are stated to take place "at the second network", in particular the steps of "determining" the user identity and of "generating" a user identifier. These features would be satisfied if

the steps were carried out at the "entity" of the second network at which the request was received or at any other entity or device in said second "network". Yet further entities of the second network are not implied or characterized with this feature.

5.2 The first and second networks are specified as being "operated and controlled by a service provider" and a "network operator separate" from "the service provider". What exactly it means for a "service provider" or a "network operator" to "operate and control" a network is not clear. It would seem that any service provider "operating and controlling" a network must be, *ipso facto*, a "network operator". It is not clear whether and how the fact that the network operator of the first network is also a "service provider" limits the first network or, more generally, the claimed method. Furthermore, it is not excluded by the claim language that the network operator of the second network is also a service provider, nor is it clear what difference that assumption might make for the claimed method.

5.3 Beyond that, it is noted that the operator of the first network is not mentioned anywhere else in claim 1. It is thus not clear how any property of that operator can limit the claimed method.

5.4 The operator of the second network is mentioned in the claim. It is claimed that "content protection data" being "position[ed]" at an entity of the first network must "enabl[e]" the operator of the second network "to maintain integrity of said protected content outside of said second network and within said first network in

accordance with a policy specified by an operator of said second network".

5.4.1 Irrespective of the fact that this feature is rather vague (and probably unclear in itself), it is noted that actual steps of "maintaining integrity" or enforcing a "policy" are not claimed. That is, any "content protection data" that is suitable for the claimed use would satisfy that feature irrespective of whether the operator of the second network actually uses it or in what way.

5.4.2 In the board's view, any user identification is suitable in this sense because it can be used to look up more specific (content protection) data such as encryption keys.

5.4.3 As a consequence, also the cited reference to the operator of the second network operator does not limit the claimed method.

6. The appellant argues that the fact that the second network has "authorized users" implies that the second network is a "managed network" (see the letter of 17 January 2019, page 6, paragraph 2). The board is not convinced that the term "managed network" itself has a clear meaning. The claims state that the determined "identity of [the] requesting user" establishes that the requesting user is an "authorized user of [the] second network". What exactly the authorized user is authorized to do in the second network is not claimed. For the purpose of the claimed method, it is the "unique identifier generated for [the] authorized user" - which may be and probably is different from its "identity" - which is used to identify relevant "content protection data" in the first network. The

claims do not even exclude the possibility that unique identifiers may also be generated for non-authorized users. The relevance of the claimed fact that a unique identifier is generated "for [an] authorized user" is thus unclear.

7. In summary, the board considers that the presence of the detailed language relating to two networks, its operators, its policy and the existence of authorized users, renders the claims unclear due to the fact that neither the networks nor their properties or those of their operators have any apparent impact on the claimed method. This is all the more the case, as the appellant's argument in favour of inventive step centrally relies on the allegation that D1 discloses neither a first network (see the letter of 17 January 2019, in particular page 9, paragraph 2) nor a second network as claimed, because the Internet cannot be construed as being a managed network (*loc. cit.*, page 9, paragraph 7) and that most of the amendments submitted with letter of 17 January 2019 try to establish just these differences. The features the appellant relies on in favour of inventive step being unclear and the appellant not attending the oral proceedings, the board considers it appropriate to limit its reasons to lack of clarity.

8. The board therefore concludes that claim 1 of both requests does not comply with Article 84 EPC.

9. In its preliminary opinion, the board has raised an inventive step objection based on a broad interpretation of the claimed invention. In view of the foregoing, however, the question of inventive step can be left open.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chairman:

M. Schalow W. Sekretaruk

Decision electronically authenticated