Internal distribution code:

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

Datasheet for the decision of 27 February 2024

Case Number: T 2202/21 - 3.5.03

Application Number: 16798852.6

Publication Number: 3369233

IPC: H04L29/06, G06F21/10, H04N21/258

Language of the proceedings: EN

Title of invention:
Methods and systems for managing content subscription data

Patent Proprietor:
Rovi Guides, Inc.

Opponent:
RTL Deutschland GmbH

Headword:
Managing content subscription/ROVI

Relevant legal provisions:
EPC Art. 56
RPBA 2020 Art. 12(3), 12(4)

Keyword:

Inventive step - main request (no): differences concern administrative (non-technical) aspects
Admittance of claim requests filed with the appeal - 1st and 2nd auxiliary requests (no): not sufficiently substantiated + "fresh case"

Decisions cited:

G 0001/19, T 0641/00, T 0108/20

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 2202/21 - 3.5.03

D E C I S I O N
of Technical Board of Appeal 3.5.03
of 27 February 2024

Appellant: (Opponent)	RTL Deutschland GmbH Picassoplatz 1 50679 Köln (DE)
Representative:	Springorum, Harald Kiani & Springorum Patent- und Rechtsanwälte Taubenstrasse 4 40479 Düsseldorf (DE)
Respondent: (Patent Proprietor)	Rovi Guides, Inc. 2160 Gold Street San Jose, CA 95002 (US)
Representative:	Haley Guiliano International LLP 26-28 Bedford Row London WC1R 4HE (GB)
Decision under appeal:	**Decision of the Opposition Division of the European Patent Office posted on 10 November 2021 rejecting the opposition filed against European patent No. 3369233 pursuant to Article 101(2) EPC.**

Composition of the Board:

Chair	K. Bengi-Akyürek
Members:	J. Eraso Helguera
	C. Heath

Summary of Facts and Submissions

I. This case concerns the appeal filed by the opponent (appellant) against the decision of the opposition division to reject the opposition under Article 101(2) EPC.

II. The decision under appeal mentioned *inter alia* the following prior-art document:

D2: US 8,843,736 B2.

III. Oral proceedings before the board were held on 27 February 2024.

- The appellant requested that the decision under appeal be set aside and that the patent be revoked.

- The respondent (proprietor) requested, as a **main request**, that the appeal be dismissed, i.e. that the opposition be rejected and the patent maintained as granted, or, in the alternative, that the patent be maintained in amended form on the basis of the claims of either of **two auxiliary requests** filed with the written reply to the statement of grounds of appeal.

At the end of the oral proceedings, the board's decision was announced.

IV. Claim 8 of the patent as granted (**main request**) reads as follows:

"A method for managing credential information across multiple subscription services, comprising:

receiving, at a content provider server that is associated with a first subscription service, a first authentication key from a content aggregator server that is associated with a second subscription service, wherein the first authentication key is received prior to a user subscribing to the first subscription service;
comparing the first authentication key to a first plurality of acceptable authentication keys to determine whether or not to generate a first user account for the first subscription service based on the first authentication key:

in response to determining that the first authentication key matches one of the first plurality of acceptable authentication keys, generating, at the content provider server, the first user account;
storing, at the content provider server, the first user account in a database entry that indicates that the first user account corresponds to the first authentication key;
subsequent to storing the first user account, receiving, at the content provider server, a request from the content aggregator server to subscribe the user to the first subscription service, wherein the request includes a second authentication key;
comparing the first authentication key to the second authentication key;
in response to determining that the first authentication key matches the second authentication key, validating the first user account; and

in response to validating the first user account, granting access to the first subscription service through the first user account."

Claim 7 of **auxiliary request 1** is the same as claim 8 as granted with the following addition at the end of the claim:

", wherein:
the request from the content aggregator server to subscribe the user to the first subscription service is transmitted from the content aggregation server, without further user input, in response to the user selecting a subscription level for the second subscription service at the content aggregator server; and/or,
the method further comprises transmitting, from the content provider server, a second subscription service confirmation to the content aggregator server in response to validating the first user account".

Claim 6 of **auxiliary request 2** is the same as claim 7 of auxiliary request 1 with the following addition at the end of the claim:

", the method further comprising:
receiving a second request from, the content aggregator server to access media content of the first subscription service through the first user account; and
in response to receiving the second request from the content aggregator server to access media content of the first subscription service through the first user account, creating a direct connection between the content provider server and a user equipment device (402)".

Reasons for the Decision

1. MAIN REQUEST

Claim 8 as granted comprises the following limiting features (outline used in the decision under appeal):

M8.1 A method for managing credential information across multiple subscription services, comprising:

M8.2 receiving, at a content provider server that is associated with a first subscription service, a first authentication key from a content aggregator server that is associated with a second subscription service, wherein the first authentication key is received prior to a user subscribing to the first subscription service;

M8.3 comparing the first authentication key to a first plurality of acceptable authentication keys to determine whether or not to generate a first user account for the first subscription service based on the first authentication key:

M8.4 in response to determining that the first authentication key matches one of the first plurality of acceptable authentication keys, generating, at the content provider server, the first user account;

M8.5 storing, at the content provider server, the first user account in a database entry that indicates that the first user account corresponds to the first authentication key;

M8.6 subsequent to storing the first user account, receiving, at the content provider server, a request from the content aggregator server to subscribe the user to the first subscription

service, wherein the request includes a second authentication key;

M8.7 comparing the first authentication key to the second authentication key;

M8.8 in response to determining that the first authentication key matches the second authentication key, validating the first user account; and

M8.9 in response to validating the first user account, granting access to the first subscription service through the first user account.

1.1 Claim 8 - inventive step (Articles 100(a) and 56 EPC)

Suitable starting point

1.1.1 Document **D2** concerns content and service aggregation management and serves as an appropriate starting point for the assessment of inventive step. The respondent did not challenge this. In the language of claim 8, D2 features a "content provider server" (Fig. 1: "CONTENT SERVER 34") associated with a "first subscription service" (column 3, line 59: "the portals are established by approved providers") and a "content aggregator server" (Fig. 1: "MANAGEMENT SERVER 32") associated with a "second subscription service" (column 3, lines 35 and 36: "... the CE device 12 sends account information to the management server 32").

Moreover, D2 discloses a method for managing credential information across multiple subscription services [**feature M8.1**] in which the content provider server

M8.2 receives a first authentication key ("user token") from the content aggregator server prior

to a user subscribing to the first subscription service (column 4, lines 16 and 17: "The management server 32 provides the user token ... to the content servers 34");

M8.5 stores the first user account in a database entry that indicates that the first user account corresponds to the first authentication key (column 4, lines 41 and 42: "Each content server 34 can then maintain a local database of active user tokens, ...") and receives a request from the user device (Fig. 1: "CE device 12") including a second authentication key to subscribe the user to the first subscription service (column 4, lines 43 and 44: "When a content server 34 receives a user token, ...");

M8.7 compares the first authentication key to the second authentication key (column 4, lines 44 and 45: "... it checks it against the local database of active tokens ...");

M8.8 in response to determining that the first authentication key matches the second authentication key, validates the first user account (column 4, lines 45 and 46: "... and if the user token is in the database, the logic moves to block 56 ...");

M8.9 grants access to the first subscription service through the first user account (column 4, lines 46 to 50: "... wherein the content server 34 returns a content list to the CE device 12 ...").

Distinguishing features

1.1.2 The appellant submitted that D2 explicitly referred to a "database of authorised tokens", which involved the addition of the user tokens signed using a "keyed hash"

to the database on account of a positive ascertainment of their authorisation before its introduction into the database. Thus, D2 disclosed also **features M8.3 and M8.4** whenever asymmetric encryption was used for the signing of the "keyed hashes".

1.1.3 This is not convincing. Firstly, D2 does not disclose the use of asymmetric encryption for the "hash-keying". Secondly, the appellant conflates the verification of a *public key* used to decipher a hash of a token with the matching of the *token* itself against a list of valid tokens.

1.1.4 Conversely, the respondent contended that D2 disclosed none of **features M8.3 to M8.9**. Document D2 concerned a token-based upfront payment system without "user accounts". It merely addressed the aspect of *access* to content, not the management of credentials for a *subscription* to the content. Thus, it related simply to "access control". Furthermore, the claimed method required two steps prior to granting access. First, the "first authentication key" was matched against a plurality of acceptable authentication keys to *generate* the user account [feature M8.4]. Then, the first authentication key was matched against the "second authentication key" to *validate* this user account [feature M8.8]. In D2, sending the token from the CE device to the content server did not validate it, because it had already been validated through the use of the "keyed hash".

1.1.5 These arguments do not sway the board, either. As to the existence of a "user account" in the system of D2, the board agrees with the opposition division that the storage and use of the user token may be regarded as a short-term subscription (cf. Reason 17 of the decision

under appeal, third paragraph). Claim 8 in fact does not specify which "user information" a "user account" is meant to store. And the board concurs with the appellant that the "user token" used in D2 defines a certain degree of user customisation that will not change during the respective session period (cf. D2, column 5, lines 56 to 59). With respect to the alleged "additional validation" according to feature M8.8, the board finds that the "validation of the first user account" is but a positive match of the "first and second authentication keys", i.e. a positive confirmation that the "second authentication key" indeed corresponds to one of the authentication keys previously stored at the "content provider server". In the system of D2, this validation is given by a positive match of the "user token" provided to the content server with one of the "active tokens" stored at the local database.

1.1.6 In conclusion, in agreement with the opposition division (cf. Reasons 19 of the decision under appeal), document D2 fails to disclose that:

(a) A successful comparison of the first authentication key against a plurality of acceptable authentication keys precedes the storage of the "first user account" at the content provider server [**features M8.3 and M8.4**].

(b) The content aggregator server - rather than the user equipment device ("CE device 12") - issues the request for the service including the second authentication key [**feature M8.6**].

Technical effects and objective technical problem

1.1.7 The opposition division's formulation of the objective technical problem ("management of credentials for a plurality of subscription services", cf. Reasons 21 of the decision under appeal) was not based on any particular technical effects associated with the distinguishing features previously identified. This preliminary step is however necessary in the framework of the problem-solution approach to properly assess whether or not the skilled person would have considered the introduction of these features into the system of D2. Furthermore, although credentials may have a well-recognised technical purpose *per se*, the board is not convinced that the "management of credentials" should necessarily be considered as a *technical* task rather than an *administrative* one, analogous to, for instance, maintaining an inventory of automobile spare parts.

1.1.8 The respondent submitted that, in D2, there was no hint of securely managing credential information traffic for setting up subscription accounts at the content provider servers. It defined the objective technical problem as follows:

> "To improve setting up a user subscription account with a content provider server for user access to a subscription service for content".

The technical effect of the differences was to ensure that the overall *efficiency* and *reliability* of the handling of the information for setting up a user account was improved.

1.1.9 As to **features M8.3 and M8.4**, the board considers that they could provide a reliable verification of the first authentication key on which the generated first

subscription is based. But only inasmuch as the "plurality of acceptable authentication keys" were securely obtained and handled by the content provider server - an aspect not required at all by claim 8. **Feature M8.6**, on the other hand, cannot be credibly associated with any technical aspect. In particular, the advantage derived from feature M8.6, i.e. having a (trusted) third party send the request for the service instead of the user device, is explicitly driven by *administrative* aspects rather than *technical* ones in the opposed patent (see e.g. paragraphs [0008], [0178] and [0241]). The underlying administrative (business-related) constraint could in fact be that a first subscription service enters into an agreement with a second subscription service to offer subscriptions on the first subscription service at a discounted price, thus necessitating a delegation of processing tasks from the user device to a (trusted) third party (such as a "content aggregator server").

Hence, applying the well-established COMVIK approach (cf. **T 641/00** as confirmed, for example, by **G 1/19**), the objective technical problem could be framed as "how to securely implement the above administrative concept in the system of D2, while maintaining control over the respective user accounts" (see also the opposed patent, e.g. column 53, lines 45-50 or column 68, lines 41-46).

Could-would approach

1.1.10 The respondent contended that, starting from document D2, the skilled person would have been encouraged to secure the communications between all CE devices and content servers by means, for example, of a "SSL connection" disclosed in relation to the communications between the management server and the

content server, and the management server and the CE device. This was the plain or logical thing to do in setting up a user account for a CE device as it was the CE device that was able to supply the information required to set up the account. In contrast, the "content aggregator server" of the claimed invention aggregated the credential information and implemented a trusted-party relationship that the content server could rely on to exchange messages securely and reliably. In effect, the invention was technically counter-intuitive in that it comprised *two* communication steps in setting up the user account, whereas D2 potentially only required that one communication step be performed by the CE device sending its version of the user token to the content server (i.e. at the point of sale). However, given the practicalities of the numerous CE devices of varying levels of reliability in terms of security, D2 would often have to resort to the multi-step process of having the request for content from the CE device verified by the management server. This would not change when the scheme of D2 is translated into a request to set up a *subscription*.

1.1.11 Nonetheless, the board considers that validating user accounts at a *first* subscription service (cf. e.g. D2, Fig. 1: "CONTENT SERVER 1") based on credentials of new users obtained from a *second* subscription service (cf. D2, Fig. 1: "MANAGEMENT SERVER") - as per **feature M8.6** - rather than from a user device (cf. D2, Fig. 1: "CE device 12") would have constituted a straightforward endeavour for the skilled person entrusted with the task of implementing the administrative concept of "subscription credential aggregation". In this respect, the board stresses that - irrespective of its administrative convenience - the mere use of a

(trusted) third party to manage the subscription credentials does not provide as such any additional security. Rather, such technical contribution should be derivable from the specific implementation of the communication between the concerned entities and the third party. Yet, this aspect is not present in claim 8, either.

1.1.12 As to **features M8.3 and M8.4**, in the system of D2, the authenticity of a credential is guaranteed, by way of example, with a keyed hash value (cf. D2, column 5, lines 58 and 59). Even accepting *arguendo* that the use of a pre-defined list of valid user credentials at the "content provider server" credibly contributed to the overall security (cf. point 1.1.9 above), the skilled person would have considered this possibility as a well-known alternative to the keyed hash.

1.2 It follows that the ground for opposition under Article 100(a) in conjunction with Article 56 EPC prejudices the maintenance of the patent as granted.

2. AUXILIARY REQUESTS

2.1 Each of claim 7 of **auxiliary request 1** and claim 6 of **auxiliary request 2** comprises all the limiting features of claim 8 as granted and the following additions:

M8.10 the request from the content aggregator server to subscribe the user to the first subscription service is transmitted from the content aggregator server, without further user input, in response to the user selecting a subscription level for the second subscription service at the content aggregator server [**auxiliary requests 1 and 2**] and/or,

M8.11 the method further comprises transmitting, from the content provider server, a second subscription service confirmation to the content aggregator server in response to validating the first user account [**auxiliary requests 1 and 2**],

M8.12 receiving a second request from the content aggregator server to access media content of the first subscription service through the first user account [**auxiliary request 2**];

M8.13 in response to receiving that second request, creating a direct connection between the content provider server and a user equipment device [**auxiliary request 2**].

2.2 Admittance into the appeal proceedings (Article 12 RPBA)

2.2.1 The present auxiliary requests were submitted only with the written reply to the statement of grounds of appeal. Thus, they constitute an "amendment" which may be admitted only at the discretion of the board (cf. Article 12(4) RPBA).

2.2.2 According to the respondent's written reply to the appeal (cf. pages 10 and 11), claim 1 of the present auxiliary requests is based on granted (system) claim 4 (**auxiliary requests 1 and 2**) and granted (system) claim 5 (**auxiliary request 2**), which correspond to method claims 11 and 12 as granted, respectively. The respondent further submitted that:

> "None of the prior art addresses a choice of subscription and/or a confirmation of validation of the user account." [section "Auxiliary Request #1"]

"None of the prior art addresses using a central (trusted) server to request content that is then that is then *[sic]* connected directly to the user equipment device." [section "Auxiliary Request #2"]

2.2.3 The respondent's case presented in its written reply with respect to the newly filed auxiliary requests is based on the presence of additional limitations which were never addressed by the opposition division, as can be seen from the annex to the summons, the minutes of the first-instance oral proceedings and the decision under appeal. The respondent merely asserted that "none of the prior art" - presumably the prior art cited in the opposition proceedings - addressed those additional limitations. It argued that, since the absence of features cannot be proved, this reasoning should suffice. And, at any rate, filing these claim requests before the opposition division would not have made any difference, because the opposition division's preliminary opinion had consistently been in favour of the rejection of the opposition.

2.2.4 The appellant objected that the auxiliary requests could and should have been filed already during the opposition proceedings. This would have given the appellant the possibility to react much earlier. Providing reasons during the oral proceedings before the board could hardly cure the fault in the written reply to the appeal. For this would force the appellant to build its case at a very late stage.

2.2.5 During the oral proceedings before the board, the board explained its position in regard of insufficiently substantiated claim requests. Namely that the requirement of presenting a complete case stipulated by Article 12(3) and 12(4), third sentence, RPBA is not

merely a rule of administrative convenience, but the expression of a fundamental principle of court proceedings (see **T 108/20**, Reasons 4.1, addressing procedural justice in discourse-based court proceedings).

2.2.6 Applied to this case, the board tends to agree with the respondent that a filing of auxiliary requests in opposition proceedings was not necessarily called for, as these requests would not have been dealt with during the first-instance oral proceedings or in the decision given that the patent was maintained as granted. With the opponent's appeal, new arguments were put on the table, thus calling for counter-arguments by the respondent. Counter-arguments can also consist of the filing of new claim requests where these are accompanied by corresponding arguments addressing why the alleged shortcomings of the main request would be overcome by the newly filed claim requests (cf. Article 12(3) RPBA). Where, as in the case at issue, lack of inventive step is argued, the patentee in filing new requests has not only to explain the *further* differences to prior art, but also *why* these differences are considered inventive (e.g. by applying the problem-solution approach, by arguing synergy between the additional features, etc.). It is not the task of the opponent to make the proprietor's case of inventive step in order to provide arguments against a case of (the presence of) inventive step that has not even been made, and neither is it the task of the board. The proprietor's reasoning that there were even more "distinguishing features" may provide a complete case for novelty, because novelty requires no more than one distinguishing feature. But novelty was never a ground for opposition in these proceedings. Absent any explanations as to inventive step, the discourse thus

cannot move forward because no argument in that regard has been provided. Consequently, no counter-argument can be expected and the board, as the deciding body, cannot be expected to deal with this issue. The board is therefore within its discretion not to admit the insufficiently substantiated auxiliary requests, and in the case at hand decided just so.

2.2.7 Besides, the new sets of claims constitute "fresh cases" whose admittance would necessitate an entirely new assessment by the board in regard of compliance with at least Article 52(1) EPC or even a remittal to the opposition division for further prosecution which would in turn be clearly detrimental to procedural economy.

2.3 Consequently, the board did not admit the present auxiliary requests into the appeal proceedings.

3. Since there is no allowable claim request on file, the patent must be revoked.

Order

For these reasons it is decided that:

1. The decision under appeal is set aside.

2. The patent is revoked.

The Registrar: The Chair:

B. Brückner K. Bengi-Akyürek

Decision electronically authenticated