Internal distribution code:

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

Datasheet for the decision of 5 March 2020

Case Number: T 1041/14 - 3.5.06

Application Number: 09004727.5

Publication Number: 2237182

IPC: G06F21/00

Language of the proceedings: EN

Title of invention:
Method, system, license server for providing a license to a user for accessing a protected content on a user device and software module

Applicant:
Sony DADC Austria AG

Headword:
Providing a license for accessing protected content on a user device/SONY

Relevant legal provisions:
EPC Art. 56, 84

Keyword:
Inventive step - (no)
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 1041/14 - 3.5.06

D E C I S I O N
of Technical Board of Appeal 3.5.06
of 5 March 2020

Appellant: (Applicant)	Sony DADC Austria AG Sonystraße 20 5081 Anif (AT)
Representative:	Müller Hoffmann & Partner Patentanwälte mbB St.-Martin-Straße 58 81541 München (DE)
Decision under appeal:	**Decision of the Examining Division of the European Patent Office posted on 17 December 2013 refusing European patent application No. 09004727.5 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 17 December 2013, to refuse European patent application No. 09 004 727.5 on the basis that the subject-matter of claim 1 according to the main request lacked novelty, Article 54(1,2) EPC, over the following document:

D1: US 2004/0193546 A1.

In addition, the subject-matter of claim 1 according to the first and second auxiliary requests was found to lack inventive step, Article 56 EPC, in view of D1.

II. A notice of appeal and the appeal fee were received on 22 January 2014, the appellant requesting that the decision be set aside and that the case be forwarded to the board of appeal if interlocutory revision (Article 109 EPC) was denied. Oral proceedings and a substantive communication by the board were requested if the decision could not be set aside in written proceedings.

III. With a statement of grounds of appeal, received on 2 April 2014, the appellant filed claims according to a new main and first and second auxiliary requests. The appellant requested that the decision be set aside and that a patent be granted on the basis of said new requests.

IV. In an annex to a summons to oral proceedings the board expressed its provisional opinion that the claimed subject-matter seemed to lack inventive step, Article 56 EPC, in view of D1 and also expressed doubts regarding clarity, Article 84 EPC.

V. With a letter received on 31 January 2020, the appellant submitted a new page of the description and claims according to a new main and first to fourth auxiliary requests. The appellant requested that the decision be set aside and that a patent be granted on the basis of one of said new requests. The auxiliary request for oral proceedings was maintained.

VI. At the oral proceedings, held on 5 March 2020, the appellant submitted the claims of a new main request and a new third auxiliary request, replacing the claims of the main and third auxiliary requests of 30 January 2020, respectively, both requests being withdrawn. The appellant also withdrew auxiliary request 4.

Thus the appellant's final requests were that the decision under appeal be set aside and that a patent be granted on the basis of

- claims 1 to 11 of the main request filed during the oral proceedings of 5 March 2020, or
- claims 1 to 11 of the first and second auxiliary requests filed with the letter dated 30 January 2020 or
- claims 1 to 10 of the third auxiliary request filed during the oral proceedings of 5 March 2020.

At the end of the oral proceedings the board announced its decision.

VII. The application is being considered in the following form:

Description (all requests):
page 1, received on 4 October 2011,
page 1a, received on 31 January 2020 and

pages 2 to 11, as originally filed.

Claims:
Main request: 1 to 11, received on 5 March 2020.
First auxiliary request: 1 to 11, received on 31 January 2020.
Second auxiliary request: 1 to 11, received on 31 January 2020.
Third auxiliary request: 1 to 10, received on 5 March 2020.

Drawings (all requests):
Pages 1/5 to 5/5, as originally filed.

VIII. Claim 1 according to the main request reads as follows:

"A method for providing a license to a user for accessing a purchasable protected content on a user device (200) in a system for providing a license, the protected content comprising an audio file, a video file, an e-book file, a computer game or a computer program, the method comprising: transmitting user authentication data from the user device (200) to a user account server (208); if the user authentication data corresponds to a valid user account on the user account server (208), generating a security token at the user account server (208) and transmitting the security token to the user device (200), user identification data being retrievable by means of the security token for the user account server (208), the user identification data corresponding to the system's internal data to identify a user in a user account database at the user account server (208); transmitting the security token from the user device (200) to a license server (220), the license server (220) being a server separate from the user account server (208);

transmitting the security token from the license server (220) to the user account server (208); verifying the security token at the user account server (208); if the security token has been verified, retrieving, from the user account database, the user identification data, and transmitting the user identification data from the user account server (208) to the license server (220); checking, at the license server (220), whether the user corresponding to the user identification data is entitled to the license; and transmitting a key for decrypting the protected content from the license server (220) to the user device (200), if the user identification data is validated and if the user is deemed entitled to the license."

IX. Claim 1 according to the first auxiliary request differs from that of the main request in the insertion of the expression "the security token being a session ID or a user certificate embedding a system's internal unique user ID," and in that the expression "user identification data being retrievable by means of the security token" has been amended to "user identification data being retrievable **from** the security token" (emphasis by the board).

X. Claim 1 according to the second auxiliary request differs from that of the previous auxiliary request in the addition of the expression "the user account server being an online-shop server".

XI. Claim 1 of the third auxiliary request differs from that of the main request, editorial amendments aside, in the deletion of the expression "in a system for providing a license" and the addition of the following features:

"purchasing the protected content by communication with an online shop server (300); verifying user authentication data by the online shop server (300) at a user account server (208); transmitting user identification data and protected content identification data from the online shop server (300) to the license server (220)".

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 invention relates to providing a licence to a user device, for example a smart phone (see page 3, lines 34 to 36), to allow it to play protected content, for instance an audio file or a game; see page 5, lines 18 to 20. It is known for the user to access the website of a licence provider or an online shop to purchase a key with which to access encrypted content. This approach has three disadvantages. Firstly, the user has to provide personal details to a website that they do not necessarily know or trust. Secondly, the licences are only valid for a restricted number of computers/ user devices. Thirdly, the user cannot transfer licences between user devices.

2.2 The invention aims to improve the flexibility with which a user can access protected content on different user devices; see page 1a, lines 13 to 16. As shown in

the flowchart in figure 1 (see page 3, line 15, to page 5, line 36) and the chart in figure 2, user authentication data (for instance a "login" and password) is first sent to a user account server (step S100, and arrow 3a). The user account server comprises a database containing "internal data" on each user, including user identification information, for instance a unique user ID; see page 4, lines 19 to 22. If authentication is successful (step 102 and arrow 3b), the user account server generates a "security token" and returns it to the user (arrow 3c). The requesting user presents the security token to a separate licence server (arrow 4c), which has the user account server validate it (arrows 4b and 4c). After successful validation, the user account server returns user identification information to the license server (step S104, and arrow 4d). If the so-identified user is entitled to a licence, then a licence is transmitted to the user device (step S108, and arrow 4f). The user is then allowed to access the protected content; see page 5, lines 18 to 20. The licence criteria may, for instance, restrict the number of activations within a given time frame; see the paragraph bridging pages 4 and 5. The licence is bound to the user account, rather than to the purchased content, and no user data is said to be stored in the licence server, thus protecting the confidentiality of the user data.

2.3 In the embodiment of figure 2 (see page 5, line 38, to page 7, line 23) the user device (200) has a protected application, for instance a game (202), and a separate software module (204) (shown in detail in figure 7; 700, see also page 9, lines 21 to 38) for communicating with the user account server (208) and the license server (220).

2.4 The embodiment in figure 3 (see page 7, line 25, to page 8, line 3) also relates to the user of a user device (200) purchasing a game from an online shop (300). The online shop server communicates with an account server (208) to validate the user account, and both the online shop server and the user account server communicate with a licence server (220) from which the user device retrieves a license (step 314; see page 8, lines 34 to 36).

2.5 Figure 6 shows a system for carrying out the method, comprising a user account server (208) and a licence server (220) in communication with the user device (200); see page 9, lines 1 to 19.

2.6 Claim 1 of the main request sets out a method of providing a licence to a user. Claim 1 of the first and second auxiliary requests is restricted by setting out the security token in more detail, the second auxiliary request also setting out the user account server being an online-shop server. Claim 1 of the third auxiliary request is limited with respect to that of the main request to the user account server being an online-shop server and the online shop server verifying user authentication data and transmitting data identifying the user and the protected content to the license server.

3. Claim construction

3.1 The meaning of the term "security token"

Once the user account server has confirmed the identity of (i.e. authenticated) the user, it sends a "security token" to the user device. According to page 6, lines 11 to 14, the security token can, for instance, be a

"session ID" or a "user certificate". In this context the board understands a "session ID" to be an object identifying the user only for the duration of a session. Although the description (see page 4, lines 19 to 22) refers to the possibility of a unique user ID being embedded into a larger "user certificate", the board understands a "user certificate" more broadly in this context to include an object containing *inter alia* the identity of the user.

3.2 The meaning of protected content being "purchasable"

The board takes the view that the term in claim 1 of all requests "**purchasable** protected content" (emphasis by the board) covers any encoded content protected by a DRM system (see page 11, lines 7 to 9), such as that in D1. The statement that content is "purchasable" does not imply a feature of the content itself, nor does it imply that payment is always required to access the content. It merely implies, in the present context, that the content is protected by a DRM system using encoding which **can**, **but need not**, enforce payment before granting access to the content. And, since claim 1 already implies this by mentioning licenses, the fact that content is "purchasable" is effectively redundant.

4. Document D1

4.1 D1 concerns the Digital Rights Management (DRM) of encoded, confidential contents. Once the contents have been downloaded from a contents distribution server (see [64]), they must be decoded using a key contained in a licence; see [9] and figure 4. Figure 1 gives an outline of the system, whilst figures 2 and 20 and figure 21 show the system and method, respectively, in more detail.

4.2 Each user is identified by an ID; see [65]. A user with a client computer (12, 201) authenticates themselves (203), the system (205) determining whether the user belongs to one or more groups (see [72]) specified by corresponding stored group lists; see user management server 206. If the user makes a request to access predetermined contents then an individual licence is generated by the licence distribution server (11, 205) by referring to the permission conditions stored in an access control list (ACL; 13, 206), for instance requiring membership of a certain group ([28]), and the licence is sent to the user's client computer (12, 204, 201).

4.3 The decision focused on the embodiment in figure 20 which carries out the steps illustrated in figure 21; see [140-163]. The board notes that the numbering in figure 20 of steps 1 to 9 is only used in paragraph [142] of the description. Steps 1 to 24, defined in figure 21, are different and correspond to paragraphs [145 to 161] in the description. Figure 20 gives an overview of the user authentication process in which the user communicates via the client computer (201) and sends a user ID (see [151]) via the communication plug-in (202) to the document management gateway (204) which, in turn, communicates with the user authentication server (203). The user authentication server responds with "(5) authentication verification information" and a user ID to the document management gateway (204); see figure 21, step 7 and [151]. The two user IDs are compared by the document management gateway (204); see [152]. If they match, then the user ID is sent to the licence distribution server (205) which obtains a group ID list from a user management server (206); see figure 21, steps 7/8. Using the user

ID, the group ID list and an ACL, the licence distribution server generates an individual licence (see figure 21, step 18 and [159]), which is distributed to the client (201) via the document management gateway (204); see figure 21, steps 19 and 20 and [160].

4.4 The decision (see page 7) refers to the "sockets" mentioned in D1, understood by the board to mean network sockets which enable system elements to communicate via a network. When the user makes an authentication request (see figure 21, step 1 in [145]), a direct communication link is established between a socket at the client (201) and a socket at the document management gateway (204). Once the user has been authenticated (see figure 21, step 8 and [152]), the document management gateway (204) "passes the socket of the communication of the client to the licence distribution server"; see [153]. This implies that a direct connection between the client and the licence distribution server (205) is established.

5. The main request, inventive step, Article 56 EPC

5.1 In the terms of claim 1 of the main request, D1 discloses a method for providing a licence (see figure 4) to a user for accessing a purchasable protected content on a user device (see figure 20; client 201) in a system for providing a license, the protected content comprising an audio file (see [24] "music contents"), the method comprising transmitting user authentication data (user ID; [145]) from the user device (201) to a user account server (203) (see figure 21; steps 1 to 6 and [145 to 150]), using a licence server (205) separate from the user account server (203) and checking, at the licence server (205), whether the user

corresponding to user identification data from the user account server is entitled to the licence (see step 18 and [159]).

5.2 The method according to claim 1 differs from that known from D1 in the features concerning how, once the user has been authenticated, the licence server is requested to issue the user device with a key for decrypting the protected content. In D1 the document management gateway (204) passes the user ID of the authenticated user to the licence distribution server (205); see figure 21, step 9 "Open (User ID)". However claim 1 sets out the user device being sent a security token, which the user device then presents to the licence distribution server (205) for verification by the user account server (208), as follows:

a. if the user authentication data corresponds to a valid user account on the user account server, generating a security token at the user account server and transmitting the security token to the user device;

b. user identification data being retrievable by means of the security token for the user account server, the user identification data corresponding to the system's internal data to identify a user in a user account database at the user account server;

c. transmitting the security token from the user device to the license server;

d. transmitting the security token from the license server to the user account server for verification and, if the security token has been

verified, retrieving, from a user account database at the user account server, user identification data, and transmitting the user identification data from the user account server to the license server and

e. transmitting a key for decrypting the protected content from the license server to the user device, if the user identification data is validated and if the user is deemed entitled to the license.

5.3 According to the appealed decision, the problem solved by generating a security token at the user account server (see difference feature "a" above) was to provide an alternative distribution of server functions to that in D1. The claimed selection was obvious and yielded only known advantages. The transmission of a security token from the license server to the user account server for verification (see difference feature "d" above) was mainly a trust difference. In D1, the license distribution server (205) trusted the document management gateway (204) that the user-ID it received via the socket was the verified user. In claim 1, the license server did not trust the security token and thus had to ask another trusted entity, namely the user account server, to verify it. Trusting an entity or not was a business- rather than a technical decision. Hence the trust problem could be given to the skilled person as a non-technical aim to be achieved.

5.4 The appellant has argued that the claimed subject-matter also differed from the disclosure of D1 in that purchased protected content was accessed on the user device. D1, in particular [24-25], did not mention accessing purchasable protected content. The board

notes that the method of claim 1 ends with the transmission of a decryption key to the user device; claim 1 does not set out a subsequent step of accessing the content.

5.5 The appellant has argued that, starting from D1, the invention solves the problem of accessing protected content on a user device which gives greater flexibility to the user to access the protected content on different user devices. This goal is disclosed on page 5, lines 22 to 36, of the description, in which it is stated that a user obtains a licence bound only to a user account and not to the identity of the purchased content. The licence may even allow the user to access the content on an unlimited number of user devices. The board finds that the increased flexibility is not necessarily realized, already because claim 1 is not limited to the case of a security token being transmitted to more than one user device. Moreover, if every user device has to present the security token to request a device-specific license, as claim 1 requires for the only user device mentioned, the board cannot see why it would be any more flexible for every user device to request a license via the security token rather than directly.

5.6 The appellant has also argued that the security token solves the problem of allowing a license to be issued without sending personal information to the license server. However, according to claim 1, the license server must have all information necessary to determine whether the user is entitled to a license. This may, in general, be very personal information such as payment information or the user's age. The only information which the claim requires the account server to store for a user, the user identification data, is

transmitted from the account server to the license server. Also the step of verifying the security token by the user account server does not imply that the latter would process any personal information on behalf of the license server; this step could only mean that it is verified that the security token was actually issued by the user account server, irrespective of its content. Therefore, the board also does not accept that the claimed method increases privacy.

5.7 Consequently, the board finds that indirectly issuing a license to a user device via the claimed "security token" (see difference features "a" to "d"), as opposed to issuing a license to a user device directly, has no technical effect. In particular, from the user's point of view, the claimed method of providing a license does not behave noticeably differently from that of D1. These features do not even necessarily reduce the load on the license server, since the license server does not accept the security token at face value and merely forwards it to the user account server for verification. Hence, as difference features "a" to "d" do not contribute to the technical character of the invention, they cannot contribute to inventive step.

5.8 While difference features "a" to "d" concern the provision of a license, feature "e" concerns a separate problem, namely the consequences of providing a license, and so its contribution to inventive step must be considered separately. D1 discloses, in its section on related art, that it is conventionally known to protect content by encryption and to store the decryption key in the license (see [9]). Thus feature "e" is a usual measure which the skilled person filling in the gaps of the disclosure of D1 would add in an obvious manner.

5.9 It follows that none of the difference features "a" to "e" lends inventive step to the subject-matter of claim 1. Consequently claim 1 does not involve an inventive step, Article 56 EPC.

6. The first and second auxiliary requests, clarity, Article 84 EPC

6.1 Claim 1 of both requests sets out the user identification data being retrievable "from" the security token. However, it also specifies that "the user identification data" is retrieved, if the security token has been verified, from the user account server. This is inconsistent with the statement in the claim that these data can be retrieved from the security token alone, i.e. without recourse to the account server. The board considers this contradiction to render claim 1 of both requests unclear, Article 84 EPC.

6.2 Claim 1 of both requests also differs from that of the main request *inter alia* in the insertion of the expression "the security token being a session ID or a user certificate embedding a system's internal unique user ID". The board takes the view that it is unclear how a session ID can identify the user, since different user sessions will have different session IDs and hence not be attributable to the same user, for instance to enforce the license condition of a maximum number of activations within a given time frame; see page 4, line 38. Hence also this amendment to claim 1 of both requests renders it unclear, Article 84 EPC.

7. The third auxiliary request, inventive step, Article 56 EPC

7.1 Editorial amendments aside, claim 1 of the third auxiliary request differs from that of the main request in the deletion of the expression "in a system for providing a license" and the addition of the following features:

"purchasing the protected content by communication with an online shop server (300); verifying user authentication data by the online shop server (300) at a user account server (208); transmitting user identification data and protected content identification data from the online shop server (300) to the license server (220)".

7.2 The appellant has argued that D1 did not provide a springboard for the invention because it did not disclose an online shop, but rather a document management system which selectively granted access to content; see [4] and [24]. The addition of the feature from page 11, lines 7 to 9, that the user account server is an online shop server meant that the user could not trust the online shop server, in contrast to the trustworthy user authentication server (203) in D1. The problem solved was to minimise the number of entities that the user had to provide with personal data, while increasing the flexibility of the licence server for the user. The additional feature was not obvious from common general knowledge.

7.3 In the assessment of inventive step, the skilled person can start from any prior art disclosure, including D1. Moreover, in the present context the board understands the term "online shop" to include any networked access

portal for the desired content and, on this broad reading, to be compatible with the system of D1. D1 discloses content files in the form of audio files (see [24]) being managed using a DRM system, but does not disclose how the clients obtain the protected content. However the board considers that providing a suitable access portal for that purpose would have been an obvious modification for the skilled person starting from D1.

7.4 The board considers that an online shop, as construed above, or a step of "purchasing the protected content", does not necessarily require a payment step. However, assuming *arguendo* that it did, this would also have been a usual realization for the skilled person. In particular, the groups referred to in D1 (see [25]) could, for instance, be realised by the skilled person as a group of users entitled to access content for free, such as subscribers to a service, and a group of users, for instance non-subscribers, who have to pay to access content. The distinction between charging non-subscribers and not charging subscribers is a commercial aim to be achieved by the skilled person and thus unable to contribute to inventive step.

7.5 The board notes that, as stated above, neither the increased flexibility of the licence server for the user nor the increased privacy necessarily occurs, so that these effects cannot be taken into account in support of inventive step.

7.6 The appellant argued in its letter of 31 January 2020 that the invention, by transmitting user identification data and protected content identification data to the license server, made it possible to avoid storing user login data in the license server. The board considers

it obvious that the license server must know the user and the desired content to determine license entitlement, whereas there is no need for the license server to know login information (user authentication data) which may well be local to the online shop. Therefore the board considers that what is and is not transmitted according to claim 1 is obvious. Furthermore the appellant has not explained why the communication between the online shop server, user account server and license server, set out in the additional features, is inventive.

7.7 The board concludes that the additional features are unable to lend inventive step, Article 56 EPC, 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