Internal distribution code:

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

Datasheet for the decision of 20 February 2018

Case Number: T 1399/15 - 3.5.06

Application Number: 05753625.2

Publication Number: 1756695

IPC: G06F1/00

Language of the proceedings: EN

Title of invention:
SYSTEM, METHOD, AND COMPUTER PROGRAM PRODUCT FOR PROVIDING DIGITAL RIGHTS MANAGEMENT OF PROTECTED CONTENT

Applicant:
Vital Source Technologies, Inc.

Headword:
Protected content/VITAL SOURCE

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 1399/15 - 3.5.06

D E C I S I O N
of Technical Board of Appeal 3.5.06
of 20 February 2018

Appellant: (Applicant)	Vital Source Technologies, Inc. 234 Fayetteville Street, Suite 300 Raleigh, NC 27601 (US)
Representative:	Kahlhöfer, Hermann KNH Patentanwälte Kahlhöfer Neumann Rößler Heine PartG mbB Postfach 10 33 63 40024 Düsseldorf (DE)
Decision under appeal:	**Decision of the Examining Division of the European Patent Office posted on 11 February 2015 refusing European patent application No. 05753625.2 pursuant to Article 97(2) EPC.**

Composition of the Board:

Chairman	W. Sekretaruk
Members:	M. Müller
	A. Teale

Summary of Facts and Submissions

I. The appeal is against the decision of the examining division, with reasons dispatched on 11 February 2015, to refuse European patent application No. 05 753 625 for lack of inventive step over

D1: Rosenblatt B. *et al.*, "Digital Rights Management: Business and Technology", pages 79-88 and 95-96, M&T Books, 2002.

II. Notice of appeal was filed on 13 April 2015, the appeal fee being paid on the same day. A statement of grounds of appeal was received on 19 June 2015. The appellant requested that the decision be set aside and a patent be granted on the basis of claims 1-29 according to the refused main request or one of auxiliary requests 1-3, filed with the grounds of appeal.

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

"A system for providing digital rights management (DRM) of protected content, the system comprising:

a client capable of receiving at least one piece of content, wherein the client has a client user associated therewith, and wherein the at least one piece of content is encrypted with at least one encryption key regardless of any client user authorized to access the at least one piece of encrypted content;

a DRM manager capable of transferring a license file including a client identifier uniquely identifying an authorized client and the at least one encryption key to the client, the at least one encryption key being encrypted with a public key of a public key/private key pair, the private key of the public key/private key pair being provided to the client by the DRM manager

and unique to the client user associated with the client; and

wherein the client is capable of decrypting the at least one encryption key using the private key of the public key/private key pair unique to the client user, decrypting the at least one piece of content using the decrypted at least one encryption key, and accessing the decrypted at least one piece of content."

Claim 1 of auxiliary request 1 is identical to claim 1 of the main request except that the phrase "regardless of any client" is replaced by "the at least one encryption key being non-identifying of any client".

Claim 1 of auxiliary request 2 is further amended by the addition of "and non-identifying of any client" at the end of the specification of the client.

Claim 1 of auxiliary request 3 is identical to claim 1 of the main request, except that the "client" specification now reads as follows:

"a client capable of receiving a collection of content comprising a plurality of pieces ~~at least one piece~~ of content, wherein the client has a client user associated therewith, and wherein the plurality of pieces of content are encrypted with two or more different encryption keys regardless of any client user authorized to access the plurality of pieces ~~at least one piece~~ of encrypted content;".

All four requests contain further independent claims 8, 22 and 29 to, respectively, a "digital rights management (DRM) manager", a "method" and a "computer program product" "for providing digital rights management of protected content", and claim 15 to a

"client" in that context. The wording of these claims is immaterial to this decision.

IV. In an annex to a summons to oral proceedings, the board informed the appellant of its preliminary opinion that claim 1 of all request lacked inventive step over D1, Article 56 EPC 1973. A number of potential clarity problems were also mentioned, Article 84 EPC 1973.

V. In response to the summons, the appellant did not file either amendments or arguments. However, by a telefax received on 16 February 2018, the appellant indicated that it would not be represented at the oral proceedings and requested that the board decide on the basis of the documents on file. The oral proceedings were then cancelled.

Reasons for the Decision

1. The following reasons are substantially based on the board's preliminary opinion, as expressed in the annex to its summons to oral proceedings.

The invention

2. The application relates to a "Digital Rights Management" (DRM) system comprising one or more client computers, content providers ("sources") and DRM managers (see figure 1, and page 8, lines 15-17, of the description as originally filed).

2.1 Content in the sources is encrypted, typically using symmetric keys, of which there can be "one or more" for

several pieces of content. Encryption is carried out by either the source or the DRM manager "regardless of [the] users authorized to access [...] content" (see page 5, lines 15-18; page 6, lines 9-15; page 11, paragraph 2; and page 14, paragraph 1).

2.2 If a client user requests access to a piece of protected content, their authorization will be checked first by the DRM manager (see page 11, lines 19-20). An authorized client user will then receive the symmetric key required to decrypt the content (page 11, lines 20-23). This decryption key will however not be transferred in plain text but will be encrypted for the client user in question (see page 5, lines 19-23), specifically using asymmetric encryption (see page 5, line 29, to page 6, line 1). The application discloses that the key pair may be generated by the DRM manager (see page 15, lines 26-32).

The prior art

3. D1 is an excerpt from a textbook on "Digital Rights Management". It states that content is usually encrypted (see page 81, paragraph 7; figures 5-1 and 5-2) with symmetric keys (see page 95, penultimate paragraph) and that it is known to protect the symmetric keys using asymmetric encryption (*loc. cit.*). D1 also contains the statement that the generated encryption keys are "used to authenticate users and decrypt content" (see page 82, paragraph 4). To access content, a user obtains, from a license server, a license containing the keys for decrypting the content and the rights (see figures 5-1 and 5-2). The decryption itself is carried out at the client computer by a component called "DRM controller".

The decision under appeal

4. The examining division considered that the encryption of content with a symmetric key in D1 had to be assumed to be independent of individual users (see the decision, reasons 1.1). It further found there to be two differences between claim 1 of the then only request and D1, namely that the asymmetric key pair is generated by the DRM manager and that it is unique to the user (reasons 1.2). It then argued that it would be obvious to have the DRM generate the necessary symmetric key pairs (reasons 1.3) and that the use of asymmetric keys "unique to the user" solved the problem of limiting access to the content decryption key in an obvious manner (reasons 1.4).

5. The board substantially agrees with this assessment.

Claim construction

6. The appellant challenges the decision in stating that the claims did not "ask for the encryption key for encrypting the content to be symmetric" (see grounds of appeal, page 4, paragraph 7). However, the claims specify that the client is capable of decrypting the content using the decrypted *encryption* key. In the board's understanding, this implies that the encryption is symmetric. Moreover, the description discloses explicitly that the content encryption keys are symmetric (see page 5, lines 15-18), and the board is unaware of a passage in the description disclosing asymmetric encryption for the content.

7. Claim 1 specifies that the encryption key is used "regardless of any client" (main request and auxiliary

request 3) or to be "non-identifying of any client" (auxiliary requests 1 and 2). However, it is conventional that keys by themselves do not identify individual users. Typically, such an association, if desired, is expressly represented, for instance by some form of table or by binding a key to a user through the digital signature of a certification authority.

7.1 The claims do not, however, specify any data structure (table or license) or other mechanism which would bind a key pair to a user. While, arguably, the DRM manager "provid[ing]" unique keys to the users may have to maintain a suitable mapping, this seems not to be the case for the client. As a consequence, the board takes the view that at least the client claim 15 is not limited by the requirement that the key pair be "unique to the client".

7.2 The board further notes that the claims do not specify any feature that could guarantee that the encryption was (and remained) independent of individual users.

8. Claim 1 of auxiliary request 1 prescribes that the encryption key should be "non-identifying of any [authorized] client user" and claim 1 of auxiliary request 2 further adds the phrase "and non-identifying of any client". The board considers this second addition to be redundant over the first one and thus claim 1 of auxiliary requests 1 and 2 to have identical scope.

Inventive step, Article 56 EPC 1973

9. The examining division considered that symmetric keys are normally "not linked to someone" and that they are,

in D1, "not said to be linked to the user" (see reasons 1.1, b)).

9.1 The appellant contradicts the assumption that symmetric keys are generally "user-independent" (grounds of appeal, page 4, paragraph 6, and page 5, paragraph 3) and argues that D1 teaches the contrary by stating that "encryption keys [...] are used to authenticate users and decrypt content".

9.2 The board disagrees. Firstly, it shares the examining division's view that symmetric keys are, *per se*, not linked to individual users but usable by anyone having access to them. This is not to say that symmetric keys could not be "linked to someone". However, the passage in D1 fails to state how an encryption key is meant to be used "to authenticate users". The board considers that an encryption key could be used as a credential, which anyone with access to it could produce for authentication. While D1 does not disclose this option, it also does not exclude it. In other words, the board disagrees that the cited passage on page 82 of D1 teaches away from having user-independent symmetric keys.

10. In the board's view, the examining division was right to find that claim 1 of the main request differs from D1 in that

(a) the asymmetric key pair is "provided to the client by the DRM manager" and that
(b) the asymmetric key pair is unique to the user.

10.1 In the appellant's view, the finding that these differences were obvious was based on hindsight (see

grounds of appeal, e.g. page 5, paragraph 3). The board does not share this view.

10.2 As regards difference (b), the board notes that it is evident what purpose is served by encrypting a content key for a specific, authorized user, whereas the question of where the user's asymmetric key pair is generated and how it is distributed to the user appears to be essentially arbitrary. The skilled person wanting to use asymmetric encryption, as is suggested by D1, will have to set up the system that a key pair is generated and distributed to the users. The board considers it to be within the skilled person's routine competence to place these functions anywhere in the system. The board also agrees with the examining division that placing them at a "DRM manager", for instance the license server of D1, would have been an obvious choice.

10.3 Regarding difference (a), the board first notes that user-specific asymmetric key pairs are well known in the art. In fact, it is in the nature of private keys that they are and remain "private", i.e. "owned" by individuals and not shared with others. For this reason alone, the board considers that it would be obvious to use user-specific asymmetric keys. Moreover, the board agrees with the examining division that user-specific keys have the effect of limiting content access to the authorized individual while excluding others. The desire to do this is a non-technical and obvious requirement in the context of any DRM system, which the skilled person would obviously implement using the well-known user-specific asymmetric keys.

10.4 As a consequence, the board confirms the decision that claim 1 of the main request lacks inventive step over

D1, Article 56 EPC 1973. The same also applies, *mutatis mutandis*, to the other independent claims.

11. The appellant has not given any specific arguments regarding the inventive step of the auxiliary requests. In fact, the features added to claim 1 of auxiliary requests 1 and 2 appear to be meant as clarifications to further support the preceding inventive step argument. The board therefore takes the view that the above assessment also applies directly to auxiliary requests 1 and 2, showing lack of inventive step of the independent claims vis-à-vis D1.

12. The independent claims of auxiliary request 3 further specify that several pieces of content may be encrypted with "one or more different encryption keys". The immediate effect of this feature is that a user gaining access to one piece of content may still not have access to another one. The board takes the view that it would be usual to seek to have such a fine-grained user access control in the context of a DRM system. Moreover, the skilled person would know that the use of several different encryption keys would have the desired effect and thus arrive at the claimed solution in an obvious manner, Article 56 EPC 1973.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chairman:

B. Atienza Vivancos W. Sekretaruk

Decision electronically authenticated