BESCHWERDEKAMMERN DES EUROPÄISCHEN PATENTAMTS

BOARDS OF APPEAL OF THE EUROPEAN PATENT OFFICE

CHAMBRES DE RECOURS DE L'OFFICE EUROPEEN DES BREVETS

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

Datasheet for the decision of 02 April 2009

Case Number: T 1493/06 - 3.5.03

Application Number: 01926526.3

Publication Number: 1277300

IPC: H04K 1/00

Language of the proceedings: EN

Title of invention:
System and method for controlling and enforcing access rights to encrypted media

Applicant:
MACROVISION CORPORATION

Headword:
Controlling access rights to encrypted media/MACROVISION

Relevant legal provisions:
EPC Art. 56, 111(1), 113(1), 114(1)

Relevant legal provisions (EPC 1973):
EPC R. 67

Keyword:
"Inventive step (no)"
"Substantial procedural violation (no)"
"Remittal (no)"

Decisions cited:
T 0028/81, T 0111/98, T 0402/01

Catchword:
-

Europäisches Patentamt | European Patent Office | Office européen des brevets

Beschwerdekammern | Boards of Appeal | Chambres de recours

Case Number: T 1493/06 - 3.5.03

D E C I S I O N
of the Technical Board of Appeal 3.5.03
of 02 April 2009

Appellant: MACROVISION CORPORATION
2830 De La Cruz Boulevard
Santa Clara, CA 95050 (US)

Representative: Needle, Jacqueline
Beck Greener
Fulwood House
12 Fulwood Place
London WC1V 6HR (GB)

Decision under appeal: **Decision of the Examining Division of the European Patent Office posted 28 March 2006 refusing European application No. 01926526.3 pursuant to Article 97(1) EPC 1973.**

Composition of the Board:

Chairman: A. S. Clelland
Members: T. Snell
R. Moufang

Summary of Facts and Submissions

I. This appeal is against the decision of the examining division refusing European patent application No. 01926526.3, published as WO-A-01/78285 in accordance with the PCT. The decision was based on the ground that the subject-matter of claim 1 did not meet the requirement of inventive step under Article 56 EPC with respect to the disclosure of the following documents:

D1: EP-A-0773490
D3: "WIBU-KEY", User's Guide Version 2.50, July 1998
D5: "WIBU Systems Products - The WIBU-KEY Software Protection System", January 1997

Document D3 was mentioned in the supplementary European search report; D5 was cited by the examining division in a communication accompanying a summons to oral proceedings before the examining division, in which an objection of lack of inventive step based on D3 and D5 in combination with D1 was raised.

II. In a letter of reply to the summons to oral proceedings before the examining division (Rule 71a(1) EPC 1973), the applicant submitted that, as D3 and D5 were mentioned for the first time in the communication accompanying the summons, it should have been "entitled [to] a further opportunity to respond to the Examining Division's further objections in writing before being summoned to oral proceedings". The applicant announced that it would not attend the oral proceedings and concluded the letter by stating "... should the Examining Division feel it necessary, we request that

given the circumstances of this case, examination of this application should be continued on paper".

III. The examining division announced its decision to reject the application at the oral proceedings, which were held in the applicant's absence.

IV. In the statement of grounds of appeal, the appellant (applicant) requested that the impugned decision be set aside in its entirety and the application upheld on the basis of the claims "at present on file" (ie the claims refused by the examining division).

The appellant conditionally requested oral proceedings.

V. In a communication pursuant to Rule 100(2) EPC, the board gave a preliminary opinion in which, *inter alia*, issues concerning Article 52(1) in combination with Articles 54 and 56 EPC were raised in connection with claim 1 (novelty and inventive step).

In connection with these issues, by virtue of its power under Article 114(1) EPC, the board introduced the following document into the procedure:

D7: WO-A-99/17496

VI. In response to the board's communication, the appellant submitted replacement claims of a main request and an auxiliary request together with supporting arguments.

VII. In a communication accompanying a summons to oral proceedings, the board gave a preliminary opinion that, *inter alia*, the subject-matter of claim 1 of the main

and auxiliary requests did not involve an inventive step when starting out from D7 as closest prior art.

VIII. In a letter of response to the summons, the appellant announced that it would not attend the oral proceedings.

The appellant submitted that there were fundamental deficiencies apparent in the first instance proceedings, because document D7, now considered as the most relevant prior art document, had not been cited until the later stages of the appeal process, and documents D2-D6 had only been cited by the examining division with the summons to oral proceedings. In consequence, the appellant requested remittal of the case to the examining division pursuant to Article 11 RPBA.

The appellant also submitted claims of a new main request to replace all requests on file.

The appellant formulated its requests as follows:

"Our Main Request is that the application should proceed with the claims now submitted.

The decision that the enclosed claims are allowable might be made by the Board at the oral proceedings. Alternatively, the newly filed claims of the Main Request might be remitted to the Examining Division for further consideration."

IX. Oral proceedings were held on 02 April 2009 in the absence of the appellant.

Based on the written submissions, the board understood the appellant's main request to be that the decision under appeal be set aside and a patent granted on the basis of claims 1-21 received by fax on 02 March 2009, with an auxiliary request for remittal of the case to the department of first instance for further prosecution.

After due deliberation, the board announced its decision.

X. Claim 1 of the appellant's main request reads as follows:

"A user data processor (300) for providing access to a secure package (112) that has at least three secure layers requiring decryption, the user data processor comprising:

a processing device (302);

a communications device (306) connected to the processing device and arranged to receive the secure package (112) which contains a portion of a rights controlled data object (106) and control data (116);

a user program (114) running on the processing device (302) and configured to control access to the data object (106);

a user program security module (352) configured to at least partially decrypt a first secure layer (402: 414, 416) of the secure package using a user program key (115) associated with the user program;

a user key device (120) associated with a user, detachably connected to the processing device (302), and with which the user program is arranged to communicate to obtain a user key (121), the user key device (120) being arranged to restrict the use of the data object (106) to a particular user, the user key (121) being arranged to decrypt a second secure layer (404, 418) of the secure package; and

a machine key device (118) associated with the processing device (302) and with which the user program is arranged to communicate to obtain a machine key (119), the machine key device (118) being arranged to restrict the use of the data object (106) to the particular user data processor (300) obtaining the machine key (119), the machine key (119) being arranged to decrypt a third secure layer (406, 420) of the secure package."

Reasons for the Decision

1. *Remittal*

1.1 Although remittal was understood to be the appellant's auxiliary request, the board deems it expedient to consider this matter first.

1.2 Under Article 111(1) EPC, the board has the discretion to either "exercise any power within the competence of the department which was responsible for the decision appealed" (here, the examining division) or to "remit the case to that department for further prosecution".

In deciding how to exercise its discretion, the board in the present case has considered firstly whether there were "fundamental deficiencies apparent in the first instance proceedings", as alleged by the appellant, which in accordance with Article 11 RPBA would normally require remittal, ie whether a substantial procedural violation has been committed, cf. Rule 67 EPC 1973, and secondly whether due to the introduction of document D7 by the board the case should be remitted in order to preserve two instances of examination.

1.3 With respect to remittal, the appellant argued as follows:

> "During examination of this application, the Examining Division did not cite D7, which is now considered to be the most relevant prior art. Furthermore, they did not cite any of Documents D2 to D6 until they issued a Summons to oral proceedings.
>
> During examination, and preferably in the first examination report, the Examining Division should raise all relevant objections against the case so that the applicants have the opportunity to respond to those objections. Clearly this did not occur in the present case in which the most relevant piece of prior art was only raised in the later stages of the appeal process."

1.4 In the board's view, the choice of documents for inclusion in the search report is not a matter of

procedure. As observed in Decision T 28/81 (cf. point 11 of the reasons, fourth paragraph, not published), although regrettable, all documentary searches are subject to the risk of error and omission. The omission of a relevant document from a search report is a lacuna but does not qualify as a substantial procedural violation. In any case it is not clear in the present case that the failure to cite document D7 materially affected the outcome of the examining procedure, since the examining division rejected the application on the grounds of lack of inventive step in any case, based on other documents.

1.5 Further, provided that the requirements of Article 113(1) EPC are respected, the examining division has the power, conferred on it by Article 114(1) EPC, to raise new objections and to cite new documents at any stage in the procedure up to grant. In the present case, the objection of lack of inventive step based on documents D1, D3 and D5 was communicated in a summons to oral proceedings. The applicant had approximately four months to reply in writing to the new objection (Rule 71a(1) EPC 1973). In addition, the applicant could also have availed itself of the further opportunity to respond at the oral proceedings. The decision was moreover based on essentially the same reasoning as communicated to the applicant in the summons. Thus, the board considers that under the circumstances the examining division's decision complied with Article 113(1) EPC.

1.6 The board can therefore identify no fundamental deficiencies inherent in the first instance proceedings that would justify remittal under Article 11 RPBA.

1.7 As regards the introduction of document D7 of the board's own motion (Article 114(1) EPC), the board observes that it is established case law that there is no automatic right to examination before two instances (see eg T 111/98, point 1.2 of the reasons and T 402/01, first decision, points 8 and 9 of the reasons, neither published). In T 111/98, implicitly referring to the right to be heard pursuant to Article 113(1) EPC, it was considered that remittal due to the admission of a new document should rather be an exception, for example if, without remittal, a party would not have had sufficient opportunity to defend itself against an attack based on the new document. In the present case, the board introduced document D7 at an early stage in the appeal procedure in a first communication, and subsequently issued another fully reasoned objection based on document D7 in the communication accompanying the summons to oral proceedings. The board, applying the above-mentioned criterion of T 111/98, therefore considers that the appellant has had sufficient opportunity to react to the introduction of document D7, so that in the present case remittal is not necessary in order to comply with Article 113(1) EPC.

1.8 The board also takes into account that the request for remittal was filed at a late stage in the appeal procedure, ie not directly in response to the introduction of document D7, but only in response to the summons to oral proceedings. In response to the board's introduction of document D7, the appellant instead submitted claims of a main and an auxiliary request, on which the board carried out a full substantive examination. Bearing in mind the need for procedural economy, the board finds that in the present

case factors which weigh against remittal, *inter alia* the advanced state of the board's examination and the further undue delay that would result from remittal, take precedence over the principle of two instances of examination.

1.9 For the above reasons, the request for remittal of the case to the department of first instance is rejected.

2. *Appellant's absence at oral proceedings before the board of appeal*

2.1 The appellant, having been duly summoned, informed the board that it would not attend the oral proceedings. Nevertheless, the board considered it to be expedient to hold oral proceedings for reasons of procedural economy (Article 116(1) EPC).

2.2 In the board's first communication as well as in the communication accompanying the summons, an objection of lack of inventive step based on D7 as closest prior art was raised in respect of the claim 1 pending at the time. Consequently, the appellant could reasonably have expected the board to consider at the oral proceedings this issue in respect of the amended version of claim 1 filed by the appellant in response to the summons. The appellant also had to expect that the board would discuss the appellant's newly filed request for remittal of the case to the examining division.

2.3 In accordance with Article 15(3) RPBA, the board shall not be obliged to delay any step in the proceedings, including its decision, by reason only of the absence

at oral proceedings of any party duly summoned who may then be treated as relying only on its written case.

2.4 In view of the above, the board was in a position to give a decision at the oral proceedings which complied with the requirements of Article 113(1) EPC.

3. *Main request - claim 1 - inventive step (Articles 52(1) and 56 EPC)*

3.1 The present application relates to a user data processor for providing access to a secure data package. The secure data package contains a portion of a rights controlled data object, eg a digital media file. The basic idea is that access to the data object is restricted by using multiple layers of encryption. In accordance with claim 1 there are at least three layers of encryption provided by respectively a user program key associated with a user program security module, a user key associated with a user, and a machine key associated with a processing device of the data processor.

3.2 In the view of the board, document D7 represents the closest prior art as it is the only document at the board's disposal disclosing more than one layer of encryption of a rights controlled data object. This has not been disputed by the appellant.

3.3 Document D7 discloses a method of transmitting a secure data package (eg a book file, cf. page 5, lines 1-2) from a publisher to a customer, whereby the secure package can be double encrypted (cf. page 6, 3rd paragraph). A first encryption layer is provided by a

private key of a public/private key pair embedded in an output device, inaccessible to a user (cf. page 5, 2nd paragraph and the paragraph bridging pages 5 and 6). A second encryption layer is provided by a second secret key transmitted from the publisher to the customer.

3.4 Using the language of claim 1, D7 discloses a user data processor for providing access to a secure package that has secure layers requiring decryption (Fig. 3C), the user data processor comprising:

a processing device (18);

a communications device connected to the processing device and arranged to receive the [partially decrypted] secure package (page 5, last line - page 6, line 2 in combination with page 6, lines 22-26) which contains a portion of a rights controlled data object ("ready-for-print information file"; cf. page 4, last paragraph - page 5, line 3);

a user program running on the processing device and configured to control access to the data object (cf. page 6, lines 2-5);

a user key device ("ordinary PC") associated with a user, the user key device being arranged to restrict the use of the data object to a particular user, the user key being arranged to decrypt a secure layer of the secure package (cf. page 6, 3rd and 4th paragraphs); and

a machine key device associated with the processing device (cf. page 5, 2nd paragraph) and with which the

user program is arranged to communicate to obtain a machine key, the machine key device being arranged to restrict the use of the data object to the particular user data processor obtaining the machine key, the machine key being arranged to decrypt a secure layer of the secure package (cf. page 6, 1st paragraph).

3.5 The subject-matter of claim 1 differs from the disclosure of document D7 in that, as claimed:

(i) the secure package contains "control data";

(ii) the data processor receives the secure package directly rather than via the intermediary of the user key device, the user key device is detachably connected to the data processor, and the user program is arranged to communicate with the detachably connected user key device to obtain the user key, in order to decrypt the second secure layer; and

(iii) a user program security module is configured to at least partially decrypt a further secure layer of the secure package using a user program key associated with the user program.

3.6 With respect to (i): The claim places no limitations on the nature or purpose of the control data. Moreover, data transmission conventionally involves the transmission of various types of control data, eg error correction data. Hence, this feature is not considered to be relevant to inventive step. Even if the control data are interpreted in the light of the description as data which determine rules for usage of the data object, the board notes that the packaging of a data object

with rules which govern the use of the data object is indicated to be a feature of existing systems (cf. page 1, lines 21-24, relating to the "background of the invention"). Since document D7 is a system intended for the rights control of digital media, the inclusion of such control data with the data object is regarded as self-evident, eg to specify the number of printer copies that may be made.

3.7 Distinguishing subject-matter (ii) relates to the fact that in document D7 the "user key" decryption is carried out by a user key device which is "typically ... an ordinary PC that is external to the output device" (cf. page 7, line 1), apparently placed between the incoming communication line and the output device processor 18, rather than, as claimed, the whole decryption operation being under control of the user program running on the (single) processor device. Hence, the user program running on the processor 18 of document D7 does not need to obtain the user key. However, in the board's view, the skilled person starting out from document D7 would realise that a complete PC is not necessary to carry out this functionality and would in the interests of hardware economy seek to replace this PC by a dedicated decryption processor. A commonly known example of a decryption processing arrangement makes use of a dongle (cf. D3, page 12, section 1.1), or a smart card cooperating with a host processor. In fact, the board notes that document D7 already suggests the use of a dongle, albeit in connection with the machine key based decryption layer (cf. page 8, last two paragraphs). Since a smart card or dongle requires a host processor, it is self-evident, having regard to Fig. 1 of D7, to

configure the smart card or dongle to be inserted into the output device and to operate it in cooperation with processor 18. It is also well-known that the smart card or dongle may include full cryptographic functionality, or merely supply a key. The board notes that both alternatives are also proposed in the present application on page 8, line 17 to page 9, line 1. By opting for the second alternative, the skilled person would arrive without inventive step at an arrangement including all the features identified under (ii) above.

3.8 Distinguishing feature (iii) relates to the use of a third layer of encryption using a "user program key".

The problem to be solved by this feature starting out from D7 is to further restrict access to the received digital media file.

The board considers that the posing of this problem itself does not involve an inventive step, as it is a common need in the art to provide various additional levels of access restriction, for example to prevent minors from accessing adult material.

In the board's view, the skilled person who wished to solve this problem would give due regard to the principle of embedded encryption layers taught by D7 (see in particular Figs. 3A-3E), and, without the exercise of inventive skill, appreciate that the number of encryption layers is not restricted to two and can be increased according to the level of security desired.

It is also obvious that a further layer of encryption requires a further encryption key. Claim 1 however requires that the further encryption key be a "user program key associated with the user program".

In this respect it is not clear to the board in what sense a "user program key" differs from a user key or a machine key, since the user program makes use of these other keys as well as the user program key. The board therefore attaches no special significance to the nature of the user program key or the encryption it provides, and therefore concludes that the provision of a third layer of encryption based on a user program key associated with the user program does not contribute to inventive step either.

3.9 For the above reasons, the board concludes that the skilled person would, without the exercise of inventive skill, include the features of distinguishing features (i)-(iii) in the arrangement of document D7.

Consequently, the subject-matter of claim 1 does not involve an inventive step with respect to the disclosure of D7 in combination with common general knowledge, Articles 52(1) and 56 EPC.

3.10 The appellant disputes that D7 discloses a user key within the meaning of claim 1. In this connection, the appellant states in the reply to the board's first communication: "As the [second] secret key is transmitted to the same computer as the data file, any person that has access to the receiving computer will have access to the data file and the symmetric key.

There is therefore no clear association of the symmetric key with a particular user".

3.11 However in the board's view, since the second secret key of D7 is transmitted to the customer (cf. page 6, lines 19-21), ie the user, it is implicitly a key intended for restricting access to that customer/user. This key is therefore a "user key" within the meaning of claim 1. The board considers that it is not relevant to its status as a "user key" if the key is accessed, stolen or used subsequently by another person to whom the key was not issued.

3.12 With respect to inventive step, the appellant in the letter of reply to the board's first communication also argued as follows :

> "As there is no restriction in D7 about the number of times a book can be printed once it arrives at the correct destination, D7 appears to disclose a complete system with an appropriate level of security. As such, it is highly unlikely that the skilled person would seek to improve the system by adding features that would lead to the present invention.
>
> If, however, the skilled person did choose to find a way to improve the invention disclosed in D7 to arrive at the present invention, they would need to recognise the need to attach specific conditions to the data file itself and to recognise that the resulting package of the data file with usage conditions would require more

rigorous security than the encrypted data file alone.

There is, however, no suggestion at all in D7 that it may be desirable to provide with the data file additional limitations on its use. In fact, the inventors of D7 go to some lengths to supply access to chapters of a book separately to avoid misuse, rather than finding a way to restrict access to certain parts of the data file at the receiving end. The inventors of D7 have, of course, made an attempt to increase security of the data file by providing two means of encryption/decryption. However, provided a person has access to the computer to which the encrypted data file is sent, they also have access to print the contents of the data file as many times as desired. This access is clearly not restricted to a particular user."

3.13 The board understands this argument to relate essentially to the inclusion of control data with the secure package which provide rules restricting the usage of the secure data file. However, as noted above, claim 1 places no limitation on the nature of the control data. The board therefore considers that this argument has no relevance to present claim 1, but in any case disagrees that the inclusion of such rule-based control data would not be obvious (cf. paragraph 3.6 above). Furthermore, with respect to the last sentence of the above passage of the appellant's letter, the board does not agree that in D7 access is not restricted to a particular user (cf. paragraphs 3.10 and 3.11 above).

3.14 Finally, in respect of the third encryption layer, the appellant has only argued in the letter of reply to the summons that "an arrangement with three secure layers is neither disclosed nor suggested in any of the prior art". However, for the reasons given above (paragraph 3.8 above), the board has concluded that such an arrangement, although not disclosed, is obvious in the light of the prior art.

4. In view of the above, claim 1 of the appellant's main request is not allowable.

Since claim 1 of the main request is not allowable, the main request as a whole is not allowable.

As the board has decided to reject the appellant's auxiliary request for remittal, and there are no other requests, it follows that the appeal must be dismissed.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chairman:

D. Magliano A. S. Clelland