

Internal distribution code:

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

**Datasheet for the decision
of 5 November 2008**

Case Number: T 1428/05 - 3.5.05

Application Number: 02715645.4

Publication Number: 1370921

IPC: G06F 1/00

Language of the proceedings: EN

Title of invention:

Receiving device for securely storing a content item, and
playback device

Applicant:

Koninklijke Philips Electronics N.V.

Opponent:

-

Headword:

Playback device with group key/PHILIPS

Relevant legal provisions:

EPC Art. 52(1)

RPBA Art. 15(3)

Relevant legal provisions (EPC 1973):

EPC Art. 106, 107, 108, 56

Keyword:

"Inventive step (no)"

Decisions cited:

J 0010/07

Catchword:

-



Case Number: T 1428/05 - 3.5.05

D E C I S I O N
of the Technical Board of Appeal 3.5.05
of 5 November 2008

Appellant: Koninklijke Philips Electronics N.V.
Groenewoudseweg 1
NL-5621 BA Eindhoven (NL)

Representative: Groenendaal, Antonius W. M.
Philips
Intellectual Property & Standards
P.O. Box 220
NL-5600 AE Eindhoven (NL)

Decision under appeal: Decision of the Examining Division of the
European Patent Office posted 7 July 2005
refusing European application No. 02715645.4
pursuant to Article 97(1) EPC 1973.

Composition of the Board:

Chairman: D. H. Rees
Members: A. Ritzka
G. Weiss

Summary of Facts and Submissions

I. This appeal is against the decision of the examining division dispatched 7 July 2005, refusing European Patent Application No. 02715645.4 for the reason that claim 1 did not involve an inventive step having regard to the disclosure of

D1: WO 00/52558 A.

II. Notice of appeal was filed on 29 August 2005. The appeal fee was paid one day later. The statement setting out the grounds of appeal and new claims 1 to 10 were filed on 3 November 2005. The new claims 1 to 10 were submitted to replace the claims on file.

The appellant requested that the appealed decision be set aside and that the patent be granted based on "the enclosed claims 1-18". Further, an auxiliary request for oral proceedings was made.

III. On 1 August 2008 the board issued an invitation to oral proceedings scheduled to take place on 5 November 2008 accompanied by a communication. In the communication the board observed that, in the statement of 3 November 2005 setting out the grounds of appeal, it was requested that the patent be granted based on the "enclosed claims 1 to 18", whereas only claims 1 to 10 were enclosed and that the board assumed that the appeal was based on claims 1 to 10 as submitted with letter of 3 November 2005.

Further, the board expressed the preliminary view that claim 1 did not appear to involve an inventive step having regard to the disclosure of D1 and common general knowledge, or, in the alternative, having regard to the disclosure of

D2: EP 0878796 A and D1.

The receipt of the summons and the communication was acknowledged on 6 August 2008. No comments or amendments in response to the communication were received.

IV. Oral proceedings took place as scheduled on 5 November 2008. Neither the appellant nor its representative attended the hearing. The board contacted the appellant by telephone and was informed that the representative Mr. Arnoud Engelfriet, who signed the notice of appeal, was no longer an employee of the appellant and that Mr. Antonius Groenendaal, who is mentioned as representative in the file, was not available since he was travelling in the US.

After deliberation on the basis of the submissions and the request of 3 November 2005 the board announced its decision.

V. Claim 1 read as follows:

"A playback device (121) for playing a content item (102) stored on a storage medium (111), comprising playback means (305) for playing back the content item (102) in accordance with a permission in a license file (141) for the content item (102), and using a

decryption key comprised in the license file to decrypt the content item, the license file (141) being stored encrypted on the storage medium (111),

secure storage means (309) for storing one or more decryption keys inside the playback device, each decryption key being associated with a respective group of playback devices,

registration means (306) for registering a public key of a public/secret key pair associated with the playback device (121) at a remote server hereinafter referred to as Content Distribution Management System or CDMS (310), the secret key of said public/secret key pair being stored in the secure storage means (309), and for receiving in return a decryption key associated with a group of playback devices encrypted with said public key, decrypting said encrypted decryption key and storing said decryption key in the secure, storage means (309),

decoding means (302) for checking whether a stored decryption key is suitable for decrypting the encrypted license file (141), and if so,

decrypting the license file (141) using the stored decryption key and providing the decrypted license file (141) to the playback means (305)."

Reason for the Decision

1. *Admissibility*

The appeal complies of the provisions of Articles 106 to 108 EPC 1973, which are applicable according to J 0010/07, point 1 (see Fact and Submissions point II above). Therefore it is admissible.

2. *Procedural matters*

2.1 Non-attendance of oral proceedings

Neither the appellant nor its representative attended the oral proceedings which was requested by the appellant and to which the appellant was duly summoned, see Facts and Submissions point III above.

Article 15(3) RPBA stipulates that the board shall not be obliged to delay any step in the proceedings, including its decision, by reason only of the absence at the oral proceedings of any party duly summoned who may then be treated as relying only on its written case.

Thus, the board was in a position to take a decision at the end of the hearing.

2.2 Request

The board assumes that the request made in the statement setting out the grounds of appeal that "a patent be granted on the basis of the enclosed claims 1 to 18", should be read as that "a patent be granted on the basis of the enclosed claims 1 to 10", since only claims 1 to 10 were enclosed and the appellant did not comment on the corresponding observation made in the invitation.

3. *Inventive step*

3.1 Claim 1

D2 discloses an information reproducing apparatus for reproducing information recorded on a recording medium such as a DVD as part of an information distribution system which allows quick and easy distribution of digitized works and provides a digital information usage environment assuming protection by copyright, see page 3, 1st and 5th paragraph. On a recording medium, e.g. a DVD, encrypted license information and encrypted accounting object information, i.e. a content item, is stored. Accounting object information is encrypted with an encryption key $ke(1)$. License information comprises a decoding key $kd(1)$, needed for the decryption of the accounting object information, and a license condition. License information is encrypted using an encryption key ke . For decryption of the license information a decoding key kd is needed. See page 9, lines 20 to 28.

The information reproducing apparatus comprises an information storage section, a readout section, a decoder unit and a reproduction section, see page 13, lines 27 and 28. The decoder unit decodes the license information using the decoding key kd stored in advance and decides on the basis of the obtained license condition whether the decoding key $kd(1)$ for decoding the encrypted accounting information is to be output to the reproduction section, see page 13, line 35 to 37, i.e. whether a permission for playing back the content item exists. The license information comprising decoding key $kd(1)$ and the license condition corresponds to the license file of claim 1.

The reproduction section comprises a decoder section which decodes the encrypted accounting object information transferred from the readout section using the decoder key kd(1) transferred from the decoder unit. The reproduction section displays the accounting object information on a display device. See page 13, lines 46 to 50.

The information reproducing apparatus of D2 is a playback device for playing back a content item stored on a storage medium. The display device corresponds to playback means for playing back in accordance with a permission in the license file for the content item and using the decryption key comprised in the license file to decrypt the content item, the license file being stored encrypted on the storage medium.

To avoid attack on security, the decoder unit, which holds the decoding key kd and an algorithm for decoding, may be implemented as IC-chip, see page 9, line 39 and 40. This implies that the decoder unit comprises secure storage means for storing one or more decryption keys inside the playback device.

According to page 9, line 58, only a decoder unit having the decoding key kd can perform this decoding. The board understands successful or unsuccessful decoding to be checking whether a stored decryption key is suitable for decrypting the encrypted license file. Moreover, the license information may be encrypted using a master key and a master key ID as an identifier for designating the master key for decoding the license information stored on a storage medium, see page 32,

lines 48 to 50. Checking whether a stored decryption key is suitable for decrypting the encrypted license file may also be based on the master key ID.

The decoder unit corresponds to decoding means for checking whether a stored decryption key is suitable for decrypting the encrypted license file, and if so, decrypting the license file using the stored decryption key and providing the decrypted license file to the playback means.

The playback device of claim 1 differs from the information reproducing apparatus of D2 in the provision of registration means for registering a public key of a public/secret key pair associated with the playback device at a remote server, the secret key of the public/secret key pair being stored in the secure storage means, and for receiving in return a decryption key associated with a group of playback devices encrypted with the public key, decrypting the encrypted decrypting key and storing the decryption key in the secure storage means. It is novel.

The problem underlying claim 1 is said to be to provide a playback device which allows persistent control over the usage of the content item on the storage medium and also adheres to user expectations of the usage, see page 4, lines 14 to 16 of the application as published. The board understands that this implies a playback device suitable for playing back a content item stored on the storage medium enabling multi-user access.

As a similar problem arises in the system for secure information handling disclosed in D1, the skilled

person would consult this document. In the system of D1 access to information encrypted in a data set and stored on an untrusted storage device is controlled by permitting access based on client groups, see D1, page 3, second paragraph. A public group key and a matched private group key are assigned to each group, see D1, page 4, second and third paragraphs, and a value required to decrypt the information is encrypted with the public group key. The group keys and the group membership lists are maintained by a group server, see page 10, second paragraph. According to D1, page 15, second paragraph, any media may be used to implement the storage device. The skilled person would understand that the concept of group keys may be applied to access control for a content item stored on a storage medium that is to be played back on a group of playback devices.

D2 does not explicitly mention that each decoding key is associated with a group of playback devices. However, D2 at page 9, line 48 to page 10, line 5, states that only the decoder unit having the decoding key kd can perform the decoding of $kd(1)$ required for decoding the accounting object information. The skilled person would understand that, in the system of D2, if a group of end users intends to play back the content items stored on a specific storage medium on each user's information reproducing device, i.e. stand alone device playback means, decoding means and the decryption key for decrypting the license file are needed in each of the stand alone device playback means and that the decoding key kd has to be stored in each of the decoder units. This implies that secure storage

means for storing the decryption keys are provided inside the playback device.

If, in the system of D2, the decoder unit decides that the accounting object information cannot be used, the license information must be updated. The user may update the license information through the Internet contacting a network server holding the decoding key kd, see D2, page 10, lines 6 to 12. This implies that the decoding key kd may be downloaded from the network server, i.e. a remote server. Moreover, this implies the need for registration with the remote server for getting the decryption keys.

As the skilled person is aware that the decoding key kd need secure handling, see D2, page 9, line 39 to 40, it would further understand that the decoding key kd should be encrypted for downloading. The use of a public/secret key pair associated to each user's information reproducing device for the secure download of the decoding key kd is common general knowledge, see e.g. D1, page 17, last paragraph. It would be obvious to register a public key of a public/secret key pair associated with the playback device at a remote server which keeps the decryption key associated with the group of playback devices and to receive in return the decryption key associated with the group of playback devices encrypted with the playback devices public key, decrypt the encrypted decryption key and store it in the secure storage means. Thus, the implementation of the registration means lies within the normal professional activity of the skilled person.

Hence, the subject-matter of claim 1 does not involve an inventive step having regard to the disclosure of D2 and D1 and therefore does not satisfy the requirements of Article 52(1) EPC and Article 56 EPC 1973.

3.2 Claim 7

Similar arguments to those set out in point 3.1 above with respect to claim 1 apply to the computer program product of claim 7.

3.3 Dependent claims

The dependent claims do not appear to add any inventive matter.

Order

The appeal is dismissed.

Registrar:

Chairman:

K.Götz

D. Rees