Internal distribution code:

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

Datasheet for the decision of 14 November 2018

Case Number: T 1798/12 - 3.5.06

Application Number: 07103265.0

Publication Number: 1830299

IPC: G06F21/00

Language of the proceedings: EN

Title of invention:
Digital rights management system with diversified content protection process

Applicant:
Apple Inc.

Headword:

Relevant legal provisions:
EPC 1973 Art. 82

Keyword:
Unity of invention - (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 1798/12 - 3.5.06

D E C I S I O N
of Technical Board of Appeal 3.5.06
of 14 November 2018

Appellant: (Applicant)	Apple Inc. One Apple Park Way Cupertino CA 95014 (US)
Representative:	Rooney, John-Paul Withers & Rogers LLP 4 More London Riverside London SE1 2AU (GB)
Decision under appeal:	**Decision of the Examining Division of the European Patent Office posted on 5 April 2012 refusing European patent application No. 07103265.0 pursuant to Article 97(2) EPC.**

Composition of the Board:

Chairman	W. Sekretaruk
Members:	A. Teale
	S. Krischer

Summary of Facts and Submissions

I. The present European patent application No. 07 103 265.0 is a parent application having two divisionals: 10183097.4, refused under Article 123(2) EPC, no appeal having been filed, and 10183103.0, refused under Articles 56 and 84 EPC, again no appeal having been filed.

II. The appeal is against the decision, dispatched with reasons on 5 April 2012, to refuse the present application on the basis that the subject-matter of the claims according to a main and three auxiliary requests, all received on 17 February 2012, lacked inventive step, Article 56 EPC, in view of the following document:

D3: US 2002/0157002.

III. During examination proceedings an objection of lack of inventive step was raised, based on the following document:

D1: US 2005/0050345 A1.

IV. A notice of appeal and the appeal fee were received on 5 June 2012. The appellant requested cancellation of the decision in its entirety.

V. In a statement of grounds of appeal, received on 2 August 2012, the appellant requested interlocutory revision or that the decision be set aside and a patent be granted on the basis of the main and three auxiliary requests, all received on 17 February 2012, forming the basis of the decision. The appellant also made an auxiliary request for oral proceedings and requested

that proceedings regarding the divisional applications be suspended pending the outcome of the present appeal on the parent application.

VI. In an annex to a summons to oral proceedings the board set out its provisional opinion on the appeal *inter alia* that it had doubts whether the independent claims of all four requests were unitary, Article 82 EPC 1973, *a posteriori* in view of *inter alia* D1. As neither of the divisional applications was still pending, it was now no longer possible to allow the request to suspend proceedings in these cases pending the outcome of the present appeal.

VII. In a letter dated 30 October 2018 the appellant stated that it would not attend the oral proceedings, withdrew its request for oral proceedings and requested a decision on the state of the file. No amendments or further arguments were filed. The board then cancelled the oral proceedings.

VIII. The application is thus being considered in the following form:

Description (all requests):
pages 1 and 3 to 19, as originally filed, and
page 2, received on 25 February 2011.

Claims (all received on 17 February 2012 and refiled with the grounds of appeal on 2 August 2012):
Main request: 1 to 47.
First auxiliary request: 1 to 39.
Second auxiliary request: 1 to 44.
Third auxiliary request: 1 to 38.

Drawings (all requests):

Pages 1/5 to 5/5, as originally filed.

IX. Claims 1 and 37 of the main request read as follows:

"1. A diversified protection method for distributing content to a plurality of recipients by using a plurality of different integrity functions for different recipients, the method comprising: receiving (205) a request for a set of content from a recipient of the content; and characterised by identifying (215) a set of diversity indicia associated with the recipient of the content; based on the identified set of diversity indicia, selecting (220) a particular integrity function from the plurality of different integrity functions for authenticating the content; encrypting the set of content using an encryption function selected based on the identified set of diversity indicia, the encryption function different from the selected integrity function; protecting (230) the encrypted set of content by using the selected integrity function; and sending (235) the protected content from a set of server computers to the recipient, wherein the set of diversity indicia is for identifying, at the recipient, a verification function from a set of verification functions for use by the recipient to verify the integrity of the content.

37. A digital rights management (DRM) method for protecting content using a diversified security scheme that uses a plurality (315) of different security element functions (320) for different users, the method characterised by comprising: based on a first set of diversity indicia associated with a first user of a first computer, identifying, at a centralized set of DRM computers, a first set of security element functions for protecting a set of content for

distribution to the first computer, the first set of security element functions comprising at least two different security element functions identified based on the first set of diversity indicia; based on a second set of diversity indicia associated with a second user of a second computer, identifying, at a centralized set of DRM computers, a second set of security element functions for protecting the set of content for distribution to the second computer, the second set of security clement functions comprising at least two different security element functions identified based on the second set of diversity indicia; at the centralized set of DRM computers, using the identified first set of security element functions to protect (310) the set of content for distribution to the first computer; and at the centralized set of DRM computers, using the identified second set of security element functions to protect (300) the set of content for distribution to the second computer."

X. Claims 29, 34 and 28 of the first, second and third auxiliary requests, respectively, have the same wording as claim 37 of the main request.

XI. Editorial amendments aside, claim 1 according to the first auxiliary request has been restricted with respect to that of the main request by adding the features of a key management function for managing keys for encrypting the content, encrypting an encryption key used to encrypt the set of content using the key management function from the selected set of security element functions and a particular set of access functions comprising a decryption function corresponding to the encryption function used to encrypt the content, a key management function corresponding to the key management function used to

encrypt the encryption key, and a verification function corresponding to the integrity function.

XII. Editorial amendments aside, claim 1 of the second auxiliary request has been restricted with respect to that of the main request by adding the features of generating an index value for the recipient at a set of server computers, using the generated index value to select, at the set of server computers, a particular encryption function from a plurality of different encryption functions for encrypting the content, generation of index value and selection of an encryption function.

XIII. Editorial amendments aside, claim 1 according to the third auxiliary request has been restricted with respect to that of the main request by incorporating the amendments according to the first and second auxiliary requests and also adding the feature of a particular set of security element functions from a plurality of different sets of security element functions, each set of security element functions comprising an encryption function for encrypting the content.

Reasons for the Decision

1. The admissibility of the appeal

In view of the facts set out at points II to IV above, the appeal fulfills the admissibility requirements under the EPC and is consequently admissible.

2. A summary of the invention

2.1 As shown in figure 1, the application relates to a digital rights management (DRM) system for distributing content from a set of DRM servers (110) via a network (120), for instance the Internet, to users' computers (115), the content being encrypted to restrict its usage to those who have been granted a right to do so; see page 10, line 4, to page 13, line 2. The problem arises that a user, termed the "receiving party", may try to break the DRM encryption used by the "distributing party". The invention solves this problem by protecting content differently for different users; see page 2, lines 22 to 25.

2.2 According to the invention, the content for a particular user is protected based on "diversity indicia", which may be received from the user or assigned by the DRM computer. In the present context, the board understands "diversity indicia" to mean indications which differ from each other. According to page 11, lines 11 to 13, the diversity criteria include any information identifying the user, such as an account number or "address" (understood by the board as "postal address"), or the user's computer, such as a MAC address. Based on the diversity indicia, the DRM computer selects a security element to protect the content, content protection being carried out by the "protection engine" 310 shown in figure 3; see page 14, line 4, to page 16, line 20. Examples of security elements are: encryption functions used by the DRM computer, integrity functions used by the DRM computer to sign content and management functions used by the DRM computer to generate or encrypt the cryptographic keys of an encryption function. Given the security element used to protect the content, the user computer

uses a corresponding access function, for instance a decryption function, a key generation function or a verification function, to remove the protection and hence access the content; see figures 2 and 7. In particular, a verification function verifies the signature produced by an integrity function in the content protection engine (310); see page 18, lines 8 to 13. The functions of providing the protected content and providing the DRM protection for the content may be provided by separate computers.

3. Document D3

3.1 D3 relates to a domain-based DRM system, the devices in each domain sharing a common cryptographic key. Each user device registers with one or more domains, meaning that the domains can "overlap"; see figure 3.

3.2 Figure 2 illustrates the various parties involved. A domain authority (204) is responsible for registering (adding) or unregistering (removing) user devices from one or more domains. This is done by first checking that the device has valid keys and certificates, and is thus "legitimate". The domain authority then sends a legitimate device the necessary keys, certificates, domain ID (see [36] and commands needed to enrol it in a domain. In particular, the device manufacturer (208) produces user devices which are trusted in the sense that they enforce content usage rules and comprise a DRM module; see [30] and figure 8; 804. A content provider (210) creates an MP3 music file which is encrypted and associated with usage rules setting out the conditions, for instance a fee structure, under which various acts, such as playing and copying the work can be carried out; see [31]. Certificate authorities (206) are trusted third parties who, for

instance, manage the digital certificates used in a public-key digital signature scheme to guarantee that participants or devices are who they claim to be; see [33].

3.3 Content is sold by cryptographically binding it to the purchasing domain's ID, meaning that only devices registered with this domain can access the content; see [37]. In the example with three user devices, shown in figure 4, two devices are registered with a first domain (XBDA), whilst the third device is registered with another domain (ZXZP). Only devices registered with a particular domain, as illustrated in figure 5, may receive content for that domain (500); see [40]. The content can be stored in an encrypted content library (figure 4;408) or on the user devices (202).

3.4 Content can be protected using symmetric key cryptography (DES or AES) when it is being transferred between system participants; see [41], RSA public key (asymmetric) cryptography being used to provide signatures for authentication purposes. Content integrity can be preserved using a SHA-1 hash function.

3.5 Figure 7 illustrates a content package comprising a licence file (760) and an encrypted content file (770). The licence file contains a rights document (720) comprising hash values for verifying the rules and integrity of the other objects in the package; see [42]. The licence file also comprises an encoded (not "enclosed"; see [43]) rights table (730) containing pre-assigned codewords and tokens, for instance the TOKEN_KEY_ID specifying the keys needed to access the digital object, such as the content encryption key assigned to a recipient using a public key encryption algorithm; see [45]. The TOKEN_WORK_HASH contains a

hash of the encoded rights table and identifies the hash function used, the TOKEN_ERT_SIGN identifying the algorithm used to sign said hash.

4. Unity, Article 82 EPC 1973

4.1 Method claims 1 and 37 are not unitary, Article 82 EPC 1973, *a posteriori*, since their common subject-matter is

"A diversified protection method for distributing content to two recipients by using different security element functions for different recipients, the method comprising identifying a set of diversity indicia associated with each recipient of the content and, based on said set of diversity indicia, selecting a security element function to protect the distributed content."

This common subject-matter is known from D3. Figure 4 of D3 discloses the case where a single device is registered with a domain (ZXZP), meaning that purchased content is bound cryptographically to the purchasing domain's ID; see [37]. Hence the cryptographic binding used for portable device 2, registered to domain ID "XBDA", differs from that used for portable device 3, registered to domain ID "ZXZP"; see [40]. The board regards the different cryptographic bindings as different "security element functions" in the sense of the claims. Each portable device in D3 is identified by a key providing unique identification (see [30]), such keys being provided to the domain authority when the devices are registered to a particular domain ID; see [29].

4.2 In the terminology of Rule 30(1) EPC 1973, there are no "special technical features" which claims 1 and 37 have in common.

4.3 Claim 29 of the first auxiliary request, claim 34 of the second auxiliary request and claim 28 of the third auxiliary request have the same wording as claim 37 of the main request, and none of the features added to claim 1 of these auxiliary requests adds to the list of common features between claim 1 and claim 29, 34 and 28, respectively, of that request. Hence the unity objection set out above against claims 1 and 37 of the main request also applies to claims 1 and 29, 34 and 28, respectively, of the first, second and third auxiliary requests.

4.4 Hence the board finds that the claims according to the main and first, second and third auxiliary requests lacks unity, Article 82 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