BESCHWERDEKAMMERN DES EUROPÄISCHEN PATENTAMTS	**BOARDS OF APPEAL OF THE EUROPEAN PATENT OFFICE**	**CHAMBRES DE RECOURS DE L'OFFICE EUROPÉEN 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 30 September 2015

Case Number:	T 1986/12 - 3.5.06
Application Number:	07075884.2
Publication Number:	1883031
IPC:	G06F21/00
Language of the proceedings:	EN

Title of invention:
Method and system for secure network-based distribution of content

Applicant:
APPLE INC.

Headword:
Digital content distribution/APPLE

Relevant legal provisions:
EPC 1973 Art. 56

Keyword:
Inventive step - (no)

Decisions cited:

Catchword:

This datasheet is not part of the Decision.
It can be changed at any time and without notice.

Case Number: T 1986/12 - 3.5.06

DECISION
# of Technical Board of Appeal 3.5.06
of 30 September 2015

Appellant:
(Applicant)

APPLE INC.
1 Infinite Loop
Cupertino, CA 95014 (US)

Representative:

Barton, Russell Glen
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 23 April 2012 refusing European patent application No. 07075884.2 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 lies against the decision of the examining division, with reasons dated 23 April 2012, to refuse European patent application No. 07 075 884.2 for lack of inventive step of the main request over the document

D2: WO 02/01330 A,

and for lack of compliance with Article 123(2) EPC for two auxiliary requests.

II. A notice of appeal was filed on 22 June 2012, the appeal fee being paid on the same day. A statement of grounds of appeal was received on 3 September 2012. The appellant requested that the decision under appeal be set aside and that a patent be granted based on claims 1-12 according to a main request or one of four auxiliary requests filed with the grounds of appeal. The remaining pending application documents were drawing sheets 1-10 and description pages 1, 8-10 and 13-17 as originally filed, pages 2, 5-7 and 11-12, as filed with the letter of 8 June 2009, and pages 3-4, filed with the letter of 4 November 2010. The second and third auxiliary requests were filed as fallback positions should the board confirm the decision with regard to the objection under Article 123(2) EPC.

III. In an annex to a summons to oral proceedings, the board set out its preliminary opinion. It tended to agree with the appellant that the main and first to third auxiliary requests complied with Article 123(2) EPC but raised objections under Articles 84 EPC 1973 and 123(2) EPC regarding the fourth auxiliary request. As to inventive step, the board tended to share some of the appellant's objections against the interpretation of D2 in the decision, but still tended to agree with the conclusion in the decision that the claimed invention lacked inventive step in view of D2. The board also introduced a new document into the procedure pursuant to Article 114(1) EPC, namely

D3: Network Associates Inc., "An Introduction to Cryptography", Copyright 1990-2000, retrieved from (and available online, on the date of this decision, at) ftp://ftp.pgpi.org/pub/pgp/7.0/docs/english/

and raised an inventive step objection based on D3 and common knowledge.

IV. In response to the summons, with a letter dated 28 August 2015, the appellant filed a new set of claims according to a fifth auxiliary request, intended to address the board's concerns concerning the fourth auxiliary request.

V. During the oral proceedings, which were held as scheduled on 30 September 2015, the appellant withdrew the second to fourth auxiliary requests.

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

"A method (600) for encrypting and downloading a media file for use at a local machine (112, 114) from a central server machine (102, 200) via a data network (108), the central server machine having user accounts for users of the system and each user account having at least one user key assigned thereto, the central server storing user keys for each of the users of the system, the central server being coupled to media storage (110) which stores a plurality of media files, said method comprising:

identifying (604) a media file from the plurality of available media files for purchase from the central server machine, each of the media files having at least media content data;

after access to the identified media file has been purchased through online interaction of the local machine with the central server machine (102, 200) via the data network;

retrieving (608) a user key from the user keys stored at the central server, the user key being associated with a user of the local machine, and the user key being assigned to the user account for the user of the local machine;

generating (612) a content key that is substantially random or pseudo-random;

encrypting (614) the media content data of the identified media file with the content key;

encrypting (616) the content key with the user key to produce an encrypted content key;

modifying (618) the identified media file to further include a user key reference and the encrypted content key, the user key reference allowing the local machine to locate the user key and;

downloading (620) the modified media file to the local machine of the user for storage."

Claim 1 of the first auxiliary request additionally states that there are a plurality of user keys for each user. The amended preamble now refers to "[...] the central server storing respective pluralities of user keys [...]", the amended retrieving step now specifies "[...] retrieving (608) a plurality of user keys from the user keys stored at the central server, the plurality of user keys being associated with a user of the local machine, and the plurality of user keys being assigned to the user account for the user of the local machine [...]", a step of "[...] selecting a user key from the plurality of user keys;" was added and the encrypting and modifying steps now refer to the "selected user key" instead of "user key".

In claim 1 of the fifth auxiliary request the selecting step reads as follows:

"selecting a user key, wherein the selection is based on cycling through the plurality of user keys;".

All three requests also contain, in addition to an independent claim 11 to a computer readable medium, an independent system claim 12 whose wording corresponds to that of the respective independent method claim 1. In particular claim 12 of the fifth auxiliary request specifies that

"[...] the central server is operable to: [...]

selecting [sic] a user key, wherein the selection is based on cycling through the plurality of user keys;".

VII. At the end of the oral proceedings, the chairman announced the decision of the board.

Reasons for the Decision

The invention

1. The application relates to the secure delivery or distribution of purchased digital media files, such as for music or videos, from a central server to a user at a

local client machine (see description as originally filed, esp. paragraphs 1 and 2).

1.1 The central server provides "accounts" for the users of the system in which, *inter alia*, user keys are stored. The account of an individual user may contain several keys (see paragraph 38, page 9, lines 3-4 from the bottom).

1.2 Whenever a user purchases a media file, one of the user keys stored at (and retrieved from) the central server is selected. It is also disclosed that the "user keys can be rotated (e.g., cycled) for improved security" (see paragraphs 48, 57 and 64).

1.3 Then, "after the user has selected [...] one of the user keys", a "random content key" is generated and used to encrypt the "media portion of the media file" (see paragraphs 49, 58 and 65). The random key itself is encrypted with the selected user key and included in the media file transmitted to the user, together with a "user key reference" (see paragraphs 50, 59, 66 and 70).

1.4 The user, in order to utilize the media file on the client machine, needs "the appropriate user key", and "the user key reference allows the user key to be located" (see paragraphs 51, 60, 68 and 70, and figure 7, Nos. 708 and 716). Eventually, the encrypted random key is "decrypted with the user key" so-obtained and then used to decrypt the media file (see paragraph 72).

Claim construction

All requests, symmetric or asymmetric encryption?

2. According to claim 1 of the main request, "a user key" is retrieved and "the user key" is used to encrypt the content key. Included in the "modified media file" to be downloaded is "a user key reference" which is specified as "allowing the local machine to locate the user key". Claim 1 does not detail what it means to "locate the user key" and how, having located the key, decryption takes place.

2.1 During oral proceedings, the appellant argued that, according to claim 1 of the main request, the user keys had to be symmetric encryption keys because the user key reference allowed the local machine to locate "the" same key that was used for encryption, thus implying that that key was used for decryption. In this context, the appellant referred to figure 7 and the corresponding description of the decryption operation, and argued that they taught the skilled person without doubt that the decryption key had to be the same as the encryption key. In this context, the appellant stressed that the disclosure of the decryption operation had to be read in the context of the entire application and that the description of the decryption operation explicitly referred back to the encryption operation (see, in particular, paragraphs 70, "As previously noted [...]" and 72, "Again, [...]").

2.2 The board is not convinced by this argument and takes the view that the skilled person would interpret the "user key reference" as an identifier distinguishing one user key from other possible ones and *ipso facto* allowing it to be identified when needed. The board further takes the view that this does not imply symmetric encryption. Rather, any "user key reference allowing the local machine to locate" an encryption key would also be suitable for locating the decryption key when using asymmetric encryption. For example, if the user key reference were "5" and meant to identify (locate) the fifth of ten public keys known for that user, the reference "5" would also identify (locate) the corresponding private key as the appropriate decryption key.

2.3 The board therefore concludes that claim 1 of the main request leaves open whether the user keys are symmetric or asymmetric keys.

2.4 The board considers that this assessment also applies to the auxiliary requests which specify that the user key reference allows "the local machine to locate the selected user key".

3. This interpretation is consistent with the description as a whole which, in the board's judgment and contrary to the appellant's assertion, does not imply that the user keys are symmetric encryption keys. With reference to the encryption process, the description refers to "a user key reference" without defining it further (see, e.g., paragraph 50). It is with regard to the decryption process only that the user key reference is explained further. It is specified that, for decryption, "the appropriate user key will be needed" and it is *that* key, i.e. the key appropriate for decryption, that the user key reference permits locating (see, e.g., paragraph 51). Likewise, in paragraph 70 it is disclosed that "[A] user key is [...] located [...] in the client machine [...] based on the user key reference". This need not be, in the board's opinion, the encryp-

tion key but could also be a private decryption key. Also, the fact that figure 7 refers back to the preceding encryption is insufficient to imply symmetric encryption. The encryption and decryption operations are linked by the user key reference even if the same reference may identify different, albeit corresponding, keys in the two operations.

Fifth auxiliary request, cycling through user keys

4. The description states that "one of the user keys is selected" and that "[T]he user keys can be rotated (e.g. cycled) for improved security" (see, e.g., paragraph 48).

4.1 Neither "rotating" nor "cycling" is defined in the application. The board understands the description to suggest (by using "e.g.") that cycling is a special instance of rotating, but it does not explain in what way the meanings of these terms differ.

4.2 The phrase "the user key is selected" leaves open whether the key is selected by the user or the system. Elsewhere the description discloses at least the option of selection being done by the user (e.g. paragraph 49). This fact raises the question of how the "cycling" feature is to be construed in the context of the claims. For instance, if cycling were achieved by the user making choices according to a prescribed security policy, but without any system support, then the selected key would, from the system perspective, be just any key and the cycling step would not imply any system feature. One might thus find that system claim 12 is unclear due to its reference to the cycling. This issue was raised during oral proceedings but was not further pursued in view of the board's conclusion on inventive step.

4.3 In the board's view the skilled person would interpret the cited passages as specifying that the user keys are selected in some cyclic order but leaving open how this is achieved and by whom.

The prior art

5. D2 also discloses a system for protecting purchased digital content, in particular electronic books, delivered from a server to a customer to a client computer (see, *inter alia*, page 6, line 19, to page 7, line 3). It is disclosed that, according to the circumstances, different security levels may be required (see page 7, line 22, to page 9, line 5). One of these levels, referred to as "fully individualized" or "owner exclusive" (see page 8, lines 28-29), ensures that content can only be opened by a particular user (page 8, line 30, to page 9, line 1). It is also disclosed that public key encryption may be used to achieve this effect (see, e.g., page 9, lines 19-21; page 32, lines 18-24).

6. D3 explains some of the background of the popular cryptosystem PGP in its version 7.0 (see 2nd page). PGP has made cryptography services available to a broad public since its creation in 1990.

6.1 Although the copyright date (1990-2000) of D3 does not constitute a definitive publication date, the board is satisfied that D3 was made available to the public before the present priority date in 2003. This was stated in the annex to the summons to oral proceedings and not challenged by the appellant.

6.2 PGP is based on asymmetric (i.e. public key) encryption in combination with one-time only session keys (see D3, pages 16-18). That is, for each communication session, a (pseudo-)random session key is generated (see also page 46, first three paragraphs) which is used to encrypt the exchanged messages. The session key itself is exchanged using the receiver's public/private key pair.

6.3 PGP also provides support for one user having multiple private keys (and thus multiple key pairs; see page 19, 3rd paragraph).

Inventive step

7. The board agrees with the decision under appeal that D2 is a suitable starting point for assessing inventive step.

8. However, rather than starting from an individual detailed embodiment of D2, the board prefers to start from the general context described in D2, namely a client-server architecture for the purchase and distribution of digital media content, i.e. an online shop. D2 also discloses user accounts (see page 45, Users Table) which are, however, also commonly known.

8.1 In such a context, the claimed invention constitutes an "approach [...] that provides users the ease and convenience of downloading media files, while at the same time provides [sic] a secured and controlled environment to protect copyright holders' rights to the content contained within the media files" (see the present application, paragraph 5).

8.2 This idea is, in the board's view, well-known in the art and also disclosed in D2.

8.3 The board therefore considers that the objective technical problem solved by the invention over the online shop known from D2 can be seen as implementing secure delivery of digital content.

8.4 The board appreciates that D2 discloses solutions for this problem. This would however not prevent the skilled person from seeking a simpler solution than those disclosed in D2, or simply an alternative.

9. For the online shop, D2 specifically mentions the idea of owner-exclusive delivery of content. The skilled person would thus consider implementing this idea in particular.

9.1 Public key encryption was introduced *inter alia* to achieve just that: owner-exclusive delivery of messages. And PGP is a well-known and widely used tool implementing public key encryption.

9.2 It would thus have been obvious for the skilled person to consider using PGP to solve the problem posed.

9.3 The appellant has argued that the skilled person would not consider using PGP for the download of purchased media files because it was devised for secure private communication, i.e. for the exchange of private text messages.

9.4 The board agrees that this was the historical background that led to the introduction of PGP (see D3, chapter 2, starting on page 39). However, also private messages may contain media content, and media files may vary considerably in size. The board is thus not convinced that the skilled person would limit the use of PGP to certain applications or types of content as a matter of principle in view of the history of PGP; nor has the appellant convinced the board that there are any technical properties of PGP which would imply such a limitation.

10. By using PGP in the given context, the skilled person would have arrived at the invention without the exercise of an inventive step.

10.1 The use of PGP for owner-exclusive delivery requires the sender, in the given context the delivery server, to encrypt the content with the receiver's public key. Hence the key must be available via the user's identity and thus via the information available in the user accounts of the online shop. The board considers that the user's public keys are, in the terms of the claim and on a broad reading, "assigned" to the user accounts. For ease of accessibility, however, the board also regards it as obvious to store the users' public keys in their respective accounts (as is also done in D2; see again page 45).

10.2 PGP will then, for each communication session, generate a "session key" which, in the board's view, constitutes a "content key" as claimed. Furthermore, the public key with which the session key is encrypted qualifies as a user key as claimed.

10.3 The appellant has argued that the claimed content key is not a "session key" in the sense of PGP because, according to the invention, the encrypted media files are meant to be permanently stored on the user's local hard disk so that the content key remains necessary for long after the communication "session" discussed in PGP. The board does not accept this argument for three reasons. Firstly, the claims do not specify that the user permanently stores the encrypted media files. Claim 1 only specifies that the data is downloaded "for storage" but not whether the storage actually takes place and whether the intended storage is temporary or permanent. Secondly, it may also be necessary to retain the "session key" of PGP after the communication session, if users of PGP keep encrypted messages in their mail boxes. And thirdly, the application does not disclose or even hint at the encryption method being adapted for long-term storage, if desired.

10.4 The appellant's further argument that the user's public key cannot be the claimed user key because the latter must be a symmetric key did not convince the board, as explained above.

11. The use of PGP for delivering digital content in a client-server system thus covers all features of claim 1 of the main request except the use of a user key reference.

11.1 In the board's view, it is only useful to include a user key reference in the media file if "locating" the "appropriate key" is not implicit anyway, for example due to the fact that each user has only one key or key pair. If, on the other hand, there is a choice of encryption keys, then the receiver needs to know which key to use for decryption. The user key reference is an indication to this effect and thus allows the flexible use of several keys per user.

12. The board considers it obvious for users to wish to have several keys or key pairs.

12.1 For example, it may be desirable for the user to have keys of different lengths to balance efficiency and security of encryption against each other, depending, for instance, on the value of the purchased goods or on legal requirements. For instance, a short key might be prescribed for a purchase when shop and customer are located in different jurisdictions, while a long key might be allowed when the same customer is in the same jurisdiction as the shop. It is also noted that PGP anticipates the possibility of users having several private keys at the same time (see D3, p. 18, 3rd para.).

12.2 If multiple keys are available for an individual user, then one of them must be "selected", and it is obvious to make the selection result known to the receiver so that the media content can be decrypted.

12.3 Hence the board considers that it would have been obvious to include a "reference" in the downloaded file to "allow[] the local machine to locate the [pertinent] user key".

13. Summarizing, the board finds that claim 1 of the main request lacks an inventive step over D2 in combination with D3, Article 56 EPC 1973.

First auxiliary request

14. The feature added to the independent claims details the selection of a user key from a plurality of user keys. This aspect is covered by the above discussion, so that the assessment of the main request also applies to the first auxiliary request.

Fifth auxiliary request

15. The feature added to the independent claims of the fifth auxiliary request is that the user keys are

selected by cycling through them. This feature is not disclosed in either D2 or D3.

15.1 According to the problem-solution approach, the board has to determine the effect of this difference.

15.2 The description states, without further explanation, that this may be done "for improved security". During oral proceedings, the appellant explained that, due to the use of several keys, one compromised key gives access only to some but not all protected media files.

15.3 The board agrees that this is one possible advantage of using several keys. However, this effect is achieved by changing the keys, whereas the reuse of earlier keys as implied by the claimed cycling does not contribute to this effect but, in fact, limits it.

15.4 The board considers that changing keys is an obvious measure to reduce the damage of losing one key (spread the risk, don't put all your eggs in one basket). The board notes that the session keys themselves are an instance of the general idea of avoiding the repeated use of the same key.

15.5 In theory, the security gain would be maximal if no key were to ever be reused. This, however, would obviously require that new keys be generated every once in a while. The generation of new keys requires computational effort and may involve a third party (a certification authority). New keys need to be exchanged, which causes additional effort and is a security risk in itself. Moreover, an old key cannot be deleted as long as there is data encrypted with it. At some point, this might become a problem of limited memory space. Therefore, the board regards it as obvious for the skilled person that the continuous need to generate new keys is a nuisance.

15.6 The skilled person would therefore seek a trade-off between changing the user keys and having to generate too many new keys and, in the board's view without exercising an inventive step, provide a limited number of keys and change amongst them. This idea does not itself imply "cycling", since, for example, the user key could always be selected randomly from the available ones. Nonetheless, the skilled person would find cycling through the user keys an obvious way to implement the mentioned trade-off.

15.7 Therefore, the board concludes that also claim 1 of the fifth auxiliary request lacks an inventive step over D2 and D3, Article 56 EPC 1973.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chairman:

Beschwerdekammern des Europäischen Patentamts ✦ Boards of Appeal of the European Patent Office ✦ Chambres de recours de l'Office européen des brevets ✦

B. Atienza Vivancos W. Sekretaruk

Decision electronically authenticated