Internal distribution code:

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

Datasheet for the decision of 22 January 2014

Case Number: T 2431/09 - 3.5.06

Application Number: 00986345.7

Publication Number: 1242855

IPC: G06F1/00

Language of the proceedings: EN

Title of invention:
SERVER FOR AN ELECTRONIC DISTRIBUTION SYSTEM AND METHOD OF OPERATING SAME

Applicant:
MICROSOFT CORPORATION

Headword:
Electronic content distribution/MICROSOFT

Relevant legal provisions:
EPC Art. 83, 84, 56

Keyword:
Sufficiency of disclosure - main request (yes)
Claims - clarity - main request (yes)
Inventive step

Decisions cited:

Catchword:

Beschwerdekammern
Boards of Appeal
Chambres de recours

European Patent Office
D-80298 MUNICH
GERMANY
Tel. +49 (0) 89 2399-0
Fax +49 (0) 89 2399-4465

Case Number: T 2431/09 - 3.5.06

D E C I S I O N
of Technical Board of Appeal 3.5.06
of 22 January 2014

Appellant: (Applicant)	MICROSOFT CORPORATION One Microsoft Way Redmond, Washington 98052-6399 (US)
Representative:	Grünecker, Kinkeldey, Stockmair & Schwanhäusser Leopoldstrasse 4 80802 München (DE)
Decision under appeal:	**Decision of the Examining Division of the European Patent Office posted on 31 July 2009 refusing European patent application No. 00986345.7 pursuant to Article 97(2) EPC.**

Composition of the Board:

Chairman: D. Rees
Members: S. Krischer
W. Sekretaruk

Summary of Facts and Submissions

I. The appeal is directed against the decision of the examining division, posted on 31 July 2009, to refuse the application 00986345 for lack of inventive step over document:

D1 WO 96 42041 A, 27 December 1996.

II. A notice of appeal was received on 29 September 2009. The fee was received the same day. A statement of the grounds of appeal was received on 26 November 2009. Claim sets of a main and an auxiliary request were filed. Oral proceedings were requested.

III. In its summons to oral proceedings, the board gave reasons for its preliminary opinion that the application suffered from a lack of clarity of its claims (Article 84 EPC) and a lack of disclosure as to how the invention claimed was to be carried out (Article 83 EPC). Claim 1 of the auxiliary request was considered not to satisfy the requirements of Article 123(2) EPC. Furthermore, claim 1 of the two requests seemed to lack an inventive step.

IV. With a letter dated 20 December 2013, the appellant filed claim sets of a new main and of a new auxiliary request.

V. Oral proceedings were held on 22 January 2014 during which the appellant filed a claim set of a new main request. At the end of the oral proceedings, the board announced its decision.

VI. The appellant requests that the decision be set aside and a patent be granted on the basis of claims 1-23 of a main request filed during oral proceedings or claims 1-26 of an auxiliary request filed on 20 December 2013. The further text on file is: description pages 1, 3-12, 14-38, 40-58, 60, 61 as published, pages 2, 2b, 62 filed on 14 April 2005, pages 2a, 13, 39, 59 filed on 18 October 2007; drawing sheets 1-9 as published.

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

"1. A method of providing an electronic content item (10), said method comprising the acts of:

encrypting an electronic content (16) with a symmetric key (14A);

encrypting the symmetric key with a cryptographic hash of corresponding metadata (12);

embedding the encrypted symmetric key in the electronic content item;

receiving via a network, a communication, said communication comprising a uniform resource locator and originating from a first computing device (90), said uniform resource locator having information that at least identifies an electronic content item, said information including a security level indicating a level of protection required for the electronic content, said information being included in said uniform resource locator in an encrypted form;

decrypting said encrypted information;

determining said level of protection that the electronic content is to receive; and

when a given level of protection is determined,

providing (7) said electronic content item, containing said encrypted electronic content, said corresponding metadata and said encrypted symmetric key, to said first computing device."

VIII. Independent claim 21 of the main request reads as follows:

"21. A server architecture (70) adapted to deliver (7) an electronic content item (10) to client devices (90, 92), comprising:

means adapted to perform the steps of:

encrypting an electronic content (16) with a symmetric key (14A);

encrypting the symmetric key with a cryptographic hash of corresponding metadata (12); and

embedding the encrypted symmetric key in the electronic content item; and

a download server comprising:

a validation module (78) adapted to validate incoming requests for the electronic content item, wherein said incoming requests for electronic content comprise a uniform resource locator comprising at least some information in an encrypted form, wherein the

information at least identifies the electronic content item and includes a security level indicating a level of protection required for the electronic content, the validation module being further adapted to decrypt said encrypted information;

a content store module (88) adapted to determine a location (80) on the download server of the requested electronic content; and

a security level determination module adapted to determine said level of protection the electronic content is to receive,

wherein when a given level of protection is determined, the electronic content item delivered by the download server to the client devices contains said electronic content encrypted with said symmetric key, said corresponding metadata and said encrypted symmetric key."

IX. In view of the board's decision, the claim text of the auxiliary request is largely irrelevant.

Reasons for the Decision

1. *Overview*

1.1 Main request

The invention relates to a download server (78 in figures 3 and 4; claim 21 of the main request; original description page 25, lines 26-27) for electronic content (such as eBooks, video, audio, software

executables; see page 6, lines 16-19). The download server receives a download request in form of a URL (page 26, first line: "passed URL"; figure 9: 206; claim 1 of the main request, step 4) from a first computing device (e.g. PC reader 90 in figures 3, 4) of the user who has previously purchased an eBook (figure 9: 202) at a bookstore server (72 in figures 3, 4) and then received the URL (including encrypted information) from the bookstore server for downloading the eBook (page 36, lines 25-28). An example of such a URL including a download command and encrypted information can be found on page 13, lines 20-21. The mandatory and optional items in the encrypted information can be found from page 22, line 23 to page 24, line 13.

The download server then decrypts the encrypted information included in the URL (claim 1, step 5; page 25, line 29-31). This information includes in particular an eBook ID (page 25, line 32; page 22, lines 29-31; page 13, lines 7-8; claim 1, step 1) and a security level (page 23, lines 28-29; claim 1, steps 4, 6), which are used in the following steps. The download server checks the decrypted security level of the URL against a stored minimal level in order to determine the DRM protection level (page 26, lines 4-9; claim 1, steps 7).

The main request claims the procedure for the DRM protection according to what is called "*level 2*". Level 1 is without protection (page 7, lines 18-20). For level 2 eBooks ("source sealed"; page 7, lines 20-30), the content management and encryption tool (82 in figures 3, 4) encrypts the content (16 in figure 1) with a symmetric key (14A in figure 1) and

also encrypts this symmetric key 14A with a cryptographic hash of the metadata (12 in figure 1). The metadata 12 is included in the content item file (10 in figure 1). The meta-data contains the security level (page 23, lines 28-30) and the author's name (page 7, lines 28-29). This double encryption happens for all buyers in advance (see page 14, line 28 to page 15, line 3, especially the last sentence: "Tool 82 accepts clear-text source files ... and generates encrypted LIT files that are source-sealed (e.g. level 2), for later retrieval by the download server ISAPI 78."). There is no individualisation to the buyer at level 2. The download server retrieves and uploads the eBook at level 2 exactly as the tool 82 stored them in the content store 80 (page 14, lines 24-25).

1.2 Auxiliary request

Claim 1 of the auxiliary request additionally specifies "re-hashing" and "re-sealing". These are only executed at protection levels 3 and 5 (page 26, lines 13-20). Level 3 means "individually sealed" (page 7, line 30 to page 8, line 3; middle of page 60; top of page 37; page 38, paragraph 6; figure 10) and level 5 "fully individualized" (page 8, lines 21-29; page 61, line 14 to page 62, line 9). There is no explicit disclosure what happens at level 4 ("source signed"; page 8, paragraph 2; page 61, lines 6-13).

2. *Clarity and sufficient disclosure*

2.1 The objections raised in the summons (4.) concerning lack of clarity (Article 84 EPC) and insufficient disclosure (Article 83) of "sealing the electronic

content" and "sealing the content key" do not apply to the current main request, since the word "sealing" does not appear anymore therein. (Note that this is *not* the case for the *auxiliary request*.)

2.2 In some contexts the term "architecture" (claim 21) may be interpreted as an abstract mental concept. However, the present claim for a "server architecture" clearly specifies concrete, if functionally defined, means for carrying out each of the steps of the corresponding method.

2.3 Therefore, the claims of the main request are clear, and the invention as claimed therein is sufficiently disclosed.

3. *Original disclosure*

3.1 The examining division did not raise any objections to the then refused main request (identical to the former main request filed with the grounds of appeal) under Article 123(2) EPC in its decision, and the board has no reason to do so of its own motion.

3.2 As to the amendments of the former main request filed on 20 December 2013 over the former main request filed with the grounds, the board considers that the passages indicated in the marked-up version of the main request sufficiently demonstrate that these claims satisfy the requirements of Article 123(2) EPC.

3.3 The amendments of the current main request filed during oral proceedings over the former main request filed on 20 December 2013 merely represent minor clarifications. The expression "server architecture" of claim 21 can be

found on original description pages 12 and 15, lines 4-5.

3.4 Therefore, the amendments of the claims of the main request satisfy the requirements of Article 123(2) EPC.

4. *Inventiveness of the main request*

4.1 From the documents at hand, the board considers D1 to be the closest prior art, as it was in the appealed decision. This does not seem to be contested in the grounds of appeal. Neither does the board see any reason to do so.

4.2 D1 discloses a download server (called "content server", page 6, lines 11-12) for electronic content (Web pages, called "controlled files"; see page 6, lines 14-22). The download server receives a download request in form of a URL (page 6, lines 11-12) from a first computing device (called "client") of the user who has previously requested authorisation for the content at an authentication server and then received the URL including an SID (session ID) including encrypted information from the authentication server for downloading the content (page 5, line 22 to page 6, line 10). An example of such a URL for a document called "report" can be found on page 10, lines 15-25: "http://content.com/[SID]/report". The encrypted information in the SID consists of a digital signature in the form of an encrypted (cryptographic) hash of the other items in the SID (page 10, line 21, 26-30).

4.3 The download server does *not decrypt the encrypted information* included in the URL, but validates the SID by re-calculating the digital signature from the

remaining non-encrypted items in the SID and comparing the re-calculated signature with that of the SID (page 11, lines 6-12). The information identifying the content item ("http://content.com/" and "report") is also not encrypted.

4.4 There is *no security level* in the URL (including the SID) and *neither encryption of the content nor of any key*. As to the metadata in the electronic content item, it is generally known that Web pages contain some metadata, such as modification date, content type, code or (optionally) the author's name. Thus, D1 is considered to implicitly disclose metadata in content items. The board agrees with the refusal decision that refused claim 1 differs from D1 in the features listed in section 1.2 of that decision.

4.5 In addition the board also considers the *decrypting of the encrypted information in the URL* (i.e. content identifier and security level) in order to access it as a difference (see the explanation above).

4.6 With the exception of feature (viii) of "sealing the electronic content", current claim 1 contains all features found by the decision to be different from D1.

4.7 Current claim 1 further differs from D1 in

- "encrypting an electronic content (16) with a symmetric key (14A);"
- "encrypting the symmetric key with a cryptographic hash of corresponding metadata (12);"
- "embedding the encrypted symmetric key in the electronic content item;"
- "when a given level of protection is determined, providing (7) ...".

4.8 According to the appellant during the oral proceedings, the technical effect of a "method of calculating the cryptographic hash that encrypts and/or seals the symmetric key" is to "complicate/discourage tampering with the meta-data 12 contained with the eBook 10" (see original description page 9, lines 24-30). A tamperer would have to find out the above method, the kind of hash-function used, the meta-data used and the symmetric encryption algorithm in order to tamper with the meta-data. The board accepts this as a technical effect.

4.9 Nonetheless the board is not sure whether in particular these new differentiating features were considered in the search. In the original claims, which were of course the basis of that search, there was for example no mention of "encrypting the symmetric key with a cryptographic hash of corresponding metadata". Only original claims 8, 60 and 61 contain the word "hash", but use it for a completely different purpose, namely to determine whether the *encrypted information in the URL* has been tampered with, and not to encrypt the symmetric (content) key which itself is included in the content item to be downloaded by that URL.

4.10 Therefore, the board considers it to be appropriate to remit the case to the first instance in order that the examining division can decide on the inventiveness of the main request. It then has the opportunity to carry out an additional search if it finds this necessary. This proposed course of action was put to the appellant in the oral proceedings; no objection was raised.

4.11 Note that the board's provisional opinion in the summons (7.2) that "the use of a cryptographic hash of

meta-data for a similar protection is even disclosed in D1 (page 10, lines 26-30)" is not correct. In D1, the hash value of meta-data is encrypted with a symmetric key in order to add a digital signature in the URL, whereas in the claim the symmetric key is encrypted with the hash value of the meta-data (i.e. the other way around) for including this encrypted symmetric key in the content item to be downloaded by the URL.

Order

For these reasons it is decided that:

1) The decision under appeal is set aside.

2) The application is remitted to the department of first instance for further prosecution on the basis of the main request filed during the oral proceedings on 22 January 2014.

The Registrar: The Chairman:

B. Atienza Vivancos D. Rees

Decision electronically authenticated