

Internal distribution code:

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

**Datasheet for the decision
of 12 February 2009**

Case Number: T 1512/05 - 3.5.05

Application Number: 00306737.8

Publication Number: 1085394

IPC: G06F 1/00

Language of the proceedings: EN

Title of invention:
Digital data access control

Applicant:
FUJITSU LIMITED

Opponent:
-

Headword:
Digital data access control/FUJITSU

Relevant legal provisions:

Relevant legal provisions (EPC 1973):
EPC Art. 84

Keyword:
"Lack of clarity / lack of support (main and auxiliary requests)"

Decisions cited:
-

Catchword:
-



Case Number: T 1512/05 - 3.5.05

D E C I S I O N
of the Technical Board of Appeal 3.5.05
of 12 February 2009

Appellant:

FUJITSU LIMITED
1-1, Kamikodanaka 4-chome
Nakahara-ku
Kawasaki-shi
Kanagawa 211-8588 (JP)

Representative:

Stebbing, Timothy Charles
Haseltine Lake
Lincoln House
300 High Holborn
London WC1V 7JH (GB)

Decision under appeal:

Decision of the Examining Division of the
European Patent Office posted 11 July 2005
refusing European application No. 00306737.8
pursuant to Article 97(1) EPC 1973.

Composition of the Board:

Chairman: D. H. Rees
Members: P. Corcoran
F. Blumer

Summary of Facts and Submissions

- I. This is an appeal against the decision of the examining division to refuse the European patent application No. 00306737.8 published as No. 1 085 394. The decision was given in oral proceedings on 10 June 2005. Written reasons were issued on 11 July 2005.
- II. In the decision under appeal, it was found that the subject-matter of claim 1 of a main and an auxiliary request lacked inventive step in the light of the following documents:
- D1: EP 0 878 796 A;
 - D5: WO 98/42098 A;
 - D6: B. SCHNEIER: "APPLIED CRYPTOGRAPHY", Second Edition, 1996, Chapters 16 and 17, pp. 369-427, John Wiley & Sons, US, ISBN 0-471-12845-7.
- III. Notice of appeal and a statement setting out the grounds of appeal were duly filed and the appeal fee was paid. A new main request and an auxiliary request were submitted with the statement setting out the grounds of appeal. A precautionary request for oral proceedings was also made.
- IV. In a communication accompanying a summons to oral proceedings to be held on 12 February 2009 the board gave its preliminary opinion that neither of the appellant's requests were allowable. In said communication, the board raised objections under Article 84 EPC and expressed reservations as to whether the claimed invention involved an inventive step in the light of D1 and general knowledge as evidenced by the following document:

D4: B. SCHNEIER: "APPLIED CRYPTOGRAPHY", Second Edition, 1996, Chapter 15, pp. 357-368, John Wiley & Sons, US, ISBN 0-471-12845-7.

It was noted in this regard that the application as filed did not disclose any specific technical effect associated with the claimed multiple encryption/decryption other than the prevention of unauthorised access to the encrypted data. The board was therefore not convinced that the particular application of multiple encryption employed by the claimed invention involved more than the exercise of routine design skills.

V. With a telefax dated 9 February 2009, the appellant's representative informed the board that he would not be attending the scheduled oral proceedings. The appellant did not submit any substantive response in respect of the issues raised by the board in its communication.

VI. The appellant has requested that the decision under appeal be set aside and that a patent be granted on the basis of one of the following claim sets:

Claims 1-7 of the main request submitted with the statement setting out the grounds of appeal;
Claims 1-7 of the auxiliary request also submitted with the statement setting out the grounds of appeal.

The text of the description and the drawings for both requests correspond to the documents on which the decision under appeal was based, viz.:

Description, pages:

1, 2, 11-14, 16, 17, 20-22, 25-27, 31-34, 36, 38-42, 44, 45, 48 as originally filed;

3, 10, 15, 18, 19, 23, 24, 28-30, 35, 37, 43, 46, 47, 49, 51, 54, 55 as filed with the letter of 31 July 2003;

4-9, 50, 52-53 as filed with the letter of 21 July 2004.

Drawings, sheets:

1/27-27/27 as originally filed.

VII. Independent claim 1 of the main request reads as follows:

"A content access control apparatus which provides a control of access to content to be provided by an authenticated information provider to a user, said apparatus comprising:

a utilization unit (220, 230, 240; 220, 310, 240; 220, 310, 440; 520, 310, 540), said utilization unit including a medium (240, 440, 540) on which the content (241, 441, 541) is recorded; and

an access control unit (213) which controls access to the content (241, 441, 541) based on the identifying information allocated to said utilization unit and license information (242, 300, 442, 542) regarding the access to the content, wherein the license information related to the content is recorded on said medium (240, 440, 540);

said utilization unit comprising physical elements (e.g. 220, 230, and 240), including said medium, to which respective items of identifying information are allocated;

the license information (242, 300, 442, 542) recorded on said medium being formed with a combination of items of identifying information corresponding to said physical elements (e.g. 220, 230 and 240) respectively;

characterised in that

the licence information having been subjected to multiple encryption using a plurality of encryption keys by (i) encrypting a first item of identifying information with a first one of the encryption keys; (ii) encrypting a second item of identifying information together with the encrypted first item of identifying information using a second one of the encryption keys; and (iii) encrypting any further item of identifying information together with the already-encrypted items of identifying information using a further one of the encryption keys, whereby a logical product of the identifying information is set in said licence information; and in that

and [sic] said access control unit (213) allows access to the content (241, 441, 541) only when the decrypted licence information includes the same items of identifying information as those allocated to each of the physical elements of said utilization unit."

Independent claim 6 of the main request reads as follows:

"A content access control method which provide [sic] a control of access to content to be provided by an authenticated information provider to a user wherein:

the content (241, 441, 541) is recorded on a medium (240, 440, 540);

license information (242, 300, 442, 542) related to the content (241, 441, 451) is recorded on said medium;

access to the content (241, 441, 541) is controlled based on the license information (242, 300, 442, 542);

to each of physical elements (e.g. 220, 230 and 240), including said medium, used to access the content is allocated a respective item of identifying information; and

the content access control method comprises the steps of:

forming the license information recorded in the medium with a combination of items of identifying information allocated to said physical elements (220, 230, 240) respectively,

performing multiple encryption for the license information using a plurality of encryption keys by (i) encrypting a first item of identifying information with a first one of the encryption keys; (ii) encrypting a second item of identifying information together with the encrypted first item of identifying information using a second one of the encryption keys; and (iii) encrypting any further item of identifying information together with the already-encrypted items of identifying information using a further one of the encryption keys,

whereby a logical product of the identifying information is set in the license information; and

allowing access to the content (241, 441, 541) only when the decrypted license information includes the same items of identifying information as those allocated to each of the physical elements used to access the content."

Independent claim 1 of the auxiliary request reads as follows:

"A content access control apparatus which provides

a control of access to content to be provided by an authenticated information provider to a user, said apparatus comprising:

a utilization unit (220, 230, 240; 220, 310, 240; 220, 310, 440; 520, 310, 540), said utilization unit including a medium (240, 440, 540) on which the content (241, 441, 541) is recorded; and

an access control unit (213) which controls access to the content (241, 441, 541) based on the identifying information allocated to said utilization unit and license information (242, 300, 442, 542) regarding the access to the content, wherein the license information related to the content is recorded on said medium (240, 440, 540);

said utilization unit comprising physical elements (e.g. 220, 230, and 240), including said medium, to which respective items of identifying information are allocated;

the license information (242, 300, 442, 542) recorded on said medium being formed with a combination of items of identifying information corresponding to said physical elements (e.g. 220, 230 and 240) respectively; characterised in that

the apparatus is arranged to perform multiple stages of decryption upon said licence information using a plurality of encryption keys held in said utilization unit by: (i) in a first stage, decrypting the licence information with a first one of the encryption keys to obtain a first item of identifying information; (ii) in a second stage, decrypting the licence information in a

form following decryption in the first stage using a second one of the encryption keys to obtain a second item of identifying information; and (iii) in each further stage if any, decrypting the licence information in a form following decryption in the preceding stage using a further one of the encryption keys to obtain a further item of identifying information; and in that

said access control unit (213) allows access to the content (241, 441, 541) only when the items of identifying information obtained by decrypting the licence information are the same items of identifying information as those allocated to each of the physical elements of said utilization unit."

Independent claim 6 of the auxiliary request reads as follows:

"A content access control method which provide [sic] a control of access to content to be provided by an authenticated information provider to a user wherein:

the content (241, 441, 541) is recorded on a medium (240, 440, 540);

license information (242, 300, 442, 542) related to the content (241, 441, 451) is recorded on said medium;

access to the content (241, 441, 541) is controlled based on the license information (242, 300, 442, 542);

to each of physical elements (e.g. 220, 230 and 240), including said medium, used to access the content is allocated a respective item of identifying information, the license information

recorded in the medium being formed with a combination of said items of identifying information allocated to said physical elements (220, 230, 240) respectively; and

the content access control method comprises the steps of:

performing multiple stages of decryption upon said licence information using a plurality of encryption keys, possessed by said physical elements, by: (i) in a first stage, decrypting the licence information with a first one of the encryption keys to obtain a first item of identifying information; (ii) in a second stage, decrypting the licence information in a form following decryption in the first stage using a second one of the encryption keys to obtain a second item of identifying information; and (iii) in each further stage if any, decrypting the licence information in a form following decryption in the preceding stage using a further one of the encryption keys to obtain a further item of identifying information; and

allowing access to the content (241, 441, 541) only when the items of identifying information obtained by decrypting the licence information are the same items of identifying information as those allocated to each of the physical elements used to access the content.

VIII. At the end of the oral proceedings the chairman announced the board's decision.

Reasons for the Decision

1. *Main request - Article 84 EPC*

1.1 Claim 1 of the main request specifies that the licence information is "*subjected to multiple encryption using a plurality of encryption keys ... whereby a logical product of the identifying information is set in said licence information*", (cf. p.56 l.27 - p.57 l.4).

The above-cited wording of the claim is found not to comply with the requirements of Article 84 EPC for the reasons which follow.

1.1.1 The term "logical product" initially appears in the description with respect to the first embodiment, for example, in [0024] of the published application, where it is stated that "*the condition for a logical product ... is set in the AC 142*", where the AC is an access control data structure containing licence information.

As far as the board can determine, the description never states that a logical product is set in licence information but that *the condition for a logical product* is set. Hence, the expression "*a logical product of the identifying information is set in said licence information*" as used in claim 1 is unclear. To the extent that this expression can be understood, it is apparently intended to denote that an explicit indication is encoded in the licence information to specify that a plurality of conditions must be simultaneously satisfied as illustrated in Fig. 3 in relation to the first embodiment.

1.1.2 However, claim 1 is understood to be based on the second embodiment, in particular on the example using a licence information structure as illustrated in Fig.7 and described in [0062]-[0079]. Whereas it is stated in [0053] in relation to the second embodiment that the condition for a logical product is set in the licence information, the licence information structure illustrated in Fig.7 comprises no explicit indication to the effect that a plurality of conditions must be simultaneously satisfied. According to the disclosure, a plurality of licence conditions, (i.e. items of "identifying information"), are encrypted in a nested structure. These licence conditions are subsequently decrypted and checked in a sequential order as described on [0064]-[0077], cf. Fig. 9. Access to the content is only authorised if all licence conditions are satisfied.

It can be said that a logical product is evaluated in this example. However, the wording of the claim requires that a logical product is set in the licence information and the licence information structure illustrated in Fig. 7 does not contain any identifiable "logical product" set therein.

1.1.3 In the board's judgement, the limitation implied by the expression "*a logical product of the identifying information is set in said licence information*" is unclear. Insofar as this expression can be understood, it is not consistent with the passages of the description relating to the embodiment of the invention on which claim 1 is based. Hence this feature of the claim, insofar as it can be understood, is not supported by the description.

- 1.2 Claim 1 specifies that the access control unit controls access to the content "*based on the identifying information allocated to said utilization unit*" and further specifies that the utilization unit comprises physical elements "*to which respective items of identifying information are allocated*".

This wording effectively specifies two categories of identifying information, *viz.* the initially recited "identifying information" allocated to the utilization unit and the subsequently recited "items of identifying information" allocated to individual elements of the utilization unit.

Defining the matter for which protection is sought in this manner gives rise to a lack of clarity because it is not evident which features of the disclosure correspond to the initially recited "identifying information" allocated to the utilization unit. Moreover, the claim fails to define the relationship between the two categories of "identifying information". Given that the description only discloses items of "identifying information" allocated to individual elements of a utilization unit, (cf. [0053]), and there is no apparent disclosure of "identifying information" allocated to the utilization unit itself as distinct from its elements, the above-cited wording of claim 1 also lacks support by the description.

- 1.3 The objection discussed under 1.1 above applies, *mutatis mutandis*, to the corresponding feature of independent method claim 6.

1.4 Claim 7 is directed towards a computer-readable recording medium on which is recorded a program that when executed by a computer "*causes the computer to provide the content access control apparatus according to any of claims 1 to 5.*" The wording of the claim lacks semantic clarity because it is not evident what is intended by specifying that the execution of the program causes the computer to provide a content control apparatus.

1.5 In view of the foregoing, the board finds that the main request is not allowable because claims 1, 6 and 7 of said request fail to comply with the requirements of Article 84 EPC.

2. *Auxiliary request - Article 84 EPC*

2.1 The objections discussed in 1.2 and 1.4 above also apply to the corresponding claims of the auxiliary request. Hence, the auxiliary request is not allowable because claims 1 and 7 thereof fail to comply with the requirements of Article 84 EPC.

3. In the absence of an allowable request, the appeal must be dismissed.

4. *Obiter dictum*

4.1 In view of the deficiencies in the appellant's requests identified under 1. and 2. above, it is not necessary for the board to give detailed consideration to the further issues identified in the communication accompanying the

summons to oral proceedings, in particular the question of compliance with the requirements of Article 52(1) EPC. Nevertheless, for the sake of completeness, the following observations are made as an *obiter dictum*.

- 4.2 In the communication accompanying the summons to oral proceedings the board expressed its reservations concerning the matter of inventive step. In particular, it was noted that the application as filed did not disclose any specific technical effect associated with the claimed multiple encryption other than the prevention of unauthorised access to the encrypted data.
- 4.3 The appellant did not make any submissions in response to the aforementioned communication. The board therefore concludes that even if the deficiencies identified under 1. and 2. above had been remedied, the appellant could not have expected a positive finding in respect of compliance with the requirements of Article 52(1) EPC, particularly in the absence of any submissions explaining why the application of multiple encryption employed by the claimed invention should be considered to involve more than the exercise of routine design skills.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar:

The Chairman:

K. Götz

D. H. Rees