BESCHWERDEKAMMERN DES EUROPÄISCHEN PATENTAMTS

BOARDS OF APPEAL OF THE EUROPEAN PATENT OFFICE

CHAMBRES DE RECOURS DE L'OFFICE EUROPEEN 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 28 November 2012

Case Number: T 0164/09 - 3.5.06

Application Number: 02008212.9

Publication Number: 1251422

IPC: G06F 1/00

Language of the proceedings: EN

Title of invention:
Copyright protection system and method thereof

Applicant:
NEC Personal Computers, Ltd.

Headword:
Copy protection system/NEC

Relevant legal provisions (EPC 1973):
EPC Art. 56

Keyword:
"Inventive step - no"

Europäisches Patentamt | European Patent Office | Office européen des brevets

Beschwerdekammern | Boards of Appeal | Chambres de recours

Case Number: T 0164/09 - 3.5.06

D E C I S I O N
of the Technical Board of Appeal 3.5.06
of 28 November 2012

Appellant: (Applicant)
NEC Personal Computers, Ltd.
11-1, Osawki 1-chome
Shinagawa-ku
Tokyo 141-0032 (JP)

Representative:
Vossius & Partner
Siebertstrasse 4
D-81675 München (DE)

Decision under appeal: **Decision of the Examining Division of the European Patent Office posted 8 August 2008 refusing European patent application No. 02008212.9 pursuant to Article 97(2) EPC.**

Composition of the Board:

Chairman: D. H. Rees
Members: G. Zucka
W. Sekretaruk

Summary of Facts and Submissions

I. The appeal is against the decision by the examining division, with reasons dispatched on 8 August 2008, to refuse European patent application 02008212.9, on the basis that the subject-matter of the independent claim 5 in each of the three requests was not inventive, Article 56 EPC 1973. The following documents were cited in the appealed decision:

D1: EP 1 054 314 A
D2: WO 00/08909 A

II. A notice of appeal was received on 29 September 2008, the appeal fee being paid on the same day. A statement of the grounds of the appeal was received on 18 December 2008.

III. The appellant requested that the decision be set aside and a patent granted on the basis of the main request which was the subject of the refusal (re-filed with the statement of grounds) or an amended auxiliary request 1 or a new auxiliary request 2, both filed with the grounds for the appeal. The appellant made a conditional request for oral proceedings.

IV. The board issued a summons to oral proceedings. In an annex to the summons, the board set out its preliminary, negative, opinion on the appeal. The following document, illustrative of common general knowledge in the field, was introduced by the board:

D3: B. Schneier, "Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd Edition",

John Wiley & Sons, NY, US, 19 October 1995, ISBN 0-471-12845-7, pages 1 and 220 to 222

V. In reply to the summons, the appellant filed a new main and auxiliary request, replacing his previous three requests

VI. Again, illustrating the common general knowledge in the field, the following document was introduced by the board during the oral proceedings:

D4: G. Langelaar, "General description of a Pay TV system", 1999, retrieved from the Internet on 27 November 2012, URL: http://www.wirelesscommunication.nl/reference/chaptr01/brdcsyst/dvb/detpaytv.htm

VII. The appellant requests that the decision under appeal be set aside and a patent be granted on the basis of claims 1 to 8 of the main or auxiliary request received on 25 October 2012, together with description pages 1 to 36 and drawing sheets 1 to 3 as originally filed.

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

A copy protection system for encrypting input data corresponding to a work, conducting authentication for a processing device (6), being an output destination, to output the encrypted input data, and thereby, protecting a copy of said work, characterized in that said copy protection system comprises:

a broadcast reception device (1) for receiving a broadcast signal as encrypted input data;

first encrypting means (3) for, after decrypting the encrypted input data outputted from the broadcast reception device (1), inputting it, and encrypting the input data using a first cryptographic key to output the encrypted input data (A1) to first decryption means (11) of said processing device (6);

second authentication means (4) having a certificate revocation list (Dl) in which information of an invalid authentication key is described, and for generating said first cryptographic key to provide the generated first cryptographic key to said first encrypting means (3), encrypting said first cryptographic key by using an authentication key to output the encrypted first cryptographic key to first authentication means (13) of said processing device (6) on condition that mutual authentication with the first authentication means (13) of said processing device (6) based on said authentication key is completed, and disapproving said authentication in case that information of the authentication key is included in said certificate revocation list (D1), which is used for said authentication when said first cryptographic key is shared between said first encrypting means (3) and said first decryption means (11); and

certificate revocation list updating means (5) for, when receiving information of an authentication key to be invalidated which is included in the broadcast signal, said information provided together with the input data outputted from said broadcast reception device (1), of which the decryption has not been performed, updating contents of said certificate revocation list; and

said broadcast reception device (1), when receiving an authentication key for updating which is

included in the broadcast signal, said authentication key provided together with the input data of which the decryption has not been performed, outputs said authentication key for updating to authentication key updating means (14) of said processing device (6) for updating said authentication key.

Method claim 4 comprises method features corresponding to the apparatus features of claim 1.

Claim 7 relates to a program carrying out the method of claim 4.

Claim 8 relates to a data carrier storing the program of claim 7.

IX. The auxiliary request differs from the main request in that the system of claim 1 further comprises the following feature, and claim 4 comprises corresponding method steps:

second encryption means (7) for encrypting said input data using a second cryptographic key to form second cryptographic data (B1), and recording said second cryptographic data in a record medium (9)

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

Reasons for the decision

1. Reference is made to the transitional provisions in Article 1 of the Decision of the Administrative Council of 28 June 2001 on the transitional provisions under Article 7 of the Act revising the European Patent Convention of 29 November 2000, for the amended and new provisions of the EPC, from which it may be derived which Articles of the EPC 1973 are still applicable to the present application and which Articles of the EPC 2000 shall apply. As far as the Implementing Regulations are concerned, the board refers to Article 2 of the Decision of the Administrative Council of 7 December 2006 amending the Implementing Regulations of the European Patent Convention 2000.

2. *The admissibility of the appeal*

In view of the facts set out at points I and II above, the appeal is admissible, since it complies with the EPC formal admissibility requirements.

3. *Main request*

D1 discloses a copy protection system for encrypting input data corresponding to a work, conducting authentication for a processing device, being an output destination, to output the encrypted input data, and thereby, protecting a copy of said work (see D1, paragraphs 5 to 6). The system comprises:

a broadcast reception device (as set out in paragraph 55, transmission of packets of a content transmitted through several kinds of media is foreseen, which implies that the device of D1 qualifies as a

broadcast reception device at least as it is understood in the present application, *e.g.* on description page 12, lines 7 to 12) for receiving a broadcast signal as encrypted input data;

first encrypting means (24) for, after decrypting the encrypted input data outputted from the broadcast reception device, inputting it, and encrypting the input data using a first cryptographic key to output the encrypted input data to first decryption means (22) of said processing device (see paragraph [20]);

second authentication means having a certificate revocation list (column 11, lines 12 to 20) in which information of an invalid authentication key is described, and for generating said first cryptographic key to provide the generated first cryptographic key to said first encrypting means, encrypting said first cryptographic key by using an authentication key to output the encrypted first cryptographic key to first authentication means (31) of said processing device (figure 6) on condition that mutual authentication with the first authentication means of said processing device based on said authentication key is completed, and disapproving said authentication in case that information of the authentication key is included in said certificate revocation list (see column 11, lines 12 to 15: the authentication key is compared with those in the revocation list), which is used for said authentication when said first cryptographic key is shared between said first encrypting means and said first decryption means; and

certificate revocation list updating means for, when receiving information of an authentication key to be invalidated, updating contents of said certificate revocation list (see paragraph [53]).

Therefore, the following differences exist between the subject-matter of claim 1 and the system of D1:

(a) The information of the authentication key to be invalidated is provided together with the input data.

(b) The authentication key is, or at least can, be updated. (The wording of the claim leaves open at which frequency and/or under which conditions such an update takes place.)

No synergistic effect exists between features (a) and (b). Instead, they independently solve two separate problems. This fact was not contested by the appellant.

Feature (a) solves the partial problem of avoiding communication overhead. Communication overhead is a constant problem in data transmission and a skilled person is bound to try and reduce it as much as possible. One well known manner to reduce such overhead is by sending information packets together. The skilled person would, therefore, combine the sending of the information of the authentication key to be invalidated with the sending of the input data without showing any inventive activity.

As regards feature (b), it was already pointed out in the "obiter dicta", item 2.2 of the appealed decision that it is common practice in copy protection systems to update authentication keys, either to deal with a situation where an authentication key has been compromised or in the context of a regular automatic

update of the authentication key in order to improve copy protection. To support the statement that it was indeed commonplace to update authentication keys before the priority date of the application, in response to doubts expressed by the appellant, the board cited document D4 at the oral proceedings. The document, which is in fact one from a large number of documents that describe the same technology, can hardly be regarded as academic or highly specialised. Instead, it describes to a lay public how copy protection works in pay TV systems and is therefore a good illustration of common copy protection practice before the priority date of the application. In such a pay TV system, it is foreseen that authentication keys (in an "Entitlement Management Message") may be changed.

D4 mentions one common motive for updating keys, namely renewing a subscription. The board also considers that the skilled person would naturally wish to deal with a situation of relatively weak authentication keys that can be "cracked" in a relatively short time and would for that reason foresee a way to update these keys, as was common practice already before the priority date of the application. Using the disclosure of D1, he or she would find that the easiest way to carry out such an update would be by using the activation process described in paragraph [15]. The board agrees with the appellant that the word "intrinsic" in this passage implies or may imply that the authentication key is unique. However, this only means that it is unique for a given user. It does not mean that the authentication key is fixed and can not be changed. In fact, the procedure in this passage could perfectly well be applied more than once for a given user and the skilled

person would naturally foresee such a repeated application to allow an update of the authentication key, the possibility for such an update being required for the reasons set out above. Also, for the same reason as given above for feature (a), the skilled person would be led to combine the authentication key with the input data in the broadcast signal. It is furthermore noted that such a combination is commonplace, as illustrated by D4.

The skilled person would thus arrive at the subject-matter of claim 1, showing no inventive activity in the process. The main request is therefore not allowable because of a lack of inventive step, Article 56 EPC 1973.

4. *Auxiliary request*

Compared to the main request, claim 1 of the auxiliary request also contains second encryption means for encrypting said input data using a second cryptographic key to form second cryptographic data, and recording said second cryptographic data in a record medium.

The board firstly notes that it has been commonplace at least for decades to store broadcast content for later viewing (for example earlier on VHS tape systems). The board therefore does not consider it inventive to wish to provide the same feature in digital systems. The added feature solves the problem of keeping the stored data in a protected manner. It would be straightforward for the skilled person, once he or she is concerned about the security of data when it is transmitted, also to consider the security of the data when it stored. It

is well known (see, for example, D3 (which is an extract from a textbook, introduced to illustrate common knowledge in the field), page 220) that keeping stored data secure presents a different challenge than transmitting data in a secure manner. D3 (pages 221 to 222) mentions a number of encryption methods to deal with the secure storage of data. Each of these methods is designed specifically for the encryption of stored data and would be different, including the use of different keys, from the methods that are normally used to encrypt transmitted data. The skilled person would, therefore, consider the use of second encrypting means for encrypting the input data using a second cryptographic key to form second cryptographic data, and recording the second cryptographic data in a record medium, without showing any inventive activity.

The above arguments relating to the second encryption means were already made in the communication accompanying the summons to oral proceedings. The appellant presented no counter-arguments.

The auxiliary request is therefore not allowable because of a lack of inventive step, Article 56 EPC 1973.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chairman:

B. Atienza Vivancos D. H. Rees