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 7 March 2008

Case Number: T 0860/05 - 3.5.01

Application Number: 98121065.1

Publication Number: 0950941

IPC: G06F 1/00, G06F 12/14

Language of the proceedings: EN

Title of invention:
Method of and apparatus for protecting data on storage medium and storage medium

Applicant:
FUJITSU LIMITED

Opponent:
-

Headword:
Protecting data/FUJITSU

Relevant legal provisions:
-

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

Keyword:
"Inventive step - (yes) after amendment"

Decisions cited:
-

Catchword:
-

Europäisches Patentamt | European Patent Office | Office européen des brevets

Beschwerdekammern | Boards of Appeal | Chambres de recours

Case Number: T 0860/05 - 3.5.01

D E C I S I O N
of the Technical Board of Appeal 3.5.01
of 7 March 2008

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

Representative: Seeger, Wolfgang
Georg-Hager-Strasse 40
81369 München (DE)

Decision under appeal: **Decision of the Examining Division of the European Patent Office posted 24 February 2005 refusing European application No. 98121065.1 pursuant to Article 97(1) EPC 1973.**

Composition of the Board:

Chairman: S. Steinbrener
Members: W. Chandler
P. Schmitz

Summary of Facts and Submissions

I. This appeal is against the decision of the examining division to refuse the application on the ground that claim 1 of the main and first and second auxiliary requests did not involve an inventive step (Article 56 EPC 1973). The following documents were mentioned in the decision:

D1: US-A-5 677 952

D3: KAPLAN M.A.: "IBM Cryptolopes™, SuperDistribution and Digital Rights Management", IBM Research, 30 December 1996, pages 1 to 7, XP-002132994

II. In the statement setting out the grounds of appeal, the appellant requested that a patent be granted on the basis of a slightly amended set of claims.

III. In the communication accompanying the summons to oral proceedings, the Board summarised the issues to be discussed and expressed some doubts about the inventive step of the claimed subject-matter.

IV. In the response to the communication, the appellant filed a further amended main and first to third auxiliary requests.

V. At the oral proceedings, the appellant requested that the decision under appeal be set aside and that a patent be granted on the basis of claims 1 and 2 filed during the oral proceedings before the Board. At the end of the oral proceedings, the Chairman announced the decision.

VI. Claim 1 reads as follows:

"A storage medium data protecting method of protecting data on a storage medium, comprising:

an initializing process when creating a logical format, comprising inputting the user password (S1),

generating key data (PS) per logic sector on said storage medium (S2),

encrypting each key data with the password (S4), and writing all encrypted key data to the storage medium (S5), before starting encryption of the data to be protected,

a writing process corresponding to a request for writing to a logic sector on the storage medium including judging whether or not the encrypted key data have already been read out, decrypted and stored in memory (S11), and if not, reading the encrypted key data (PS'[1] to PS'[n]) corresponding to said writing request (S12), decoding said encrypted key data with said password (S13),

encrypting the data to be protected with the key data (S14), and writing the encrypted data to said logic sector on the storage medium (S15),

and a reading process corresponding to a request for reading from a logic sector on the storage medium including,

judging whether or not the encrypted key data have already been read out, decrypted and stored in memory (S21), and if not, reading the encrypted key data corresponding to said reading request (S22), decoding said encrypted key data with said password (S23),

reading the encrypted data from said logic sector on the storage medium (S24), and

decoding the data with the key data."

Apparatus claim 2 corresponds to method claim 1.

Reasons for the Decision

1. The application concerns the problem of protecting data on a storage medium. It is well known to encrypt data to be stored on a storage medium with a password (see application, Figure 15). This has the disadvantage that it provides a large amount of encrypted data that can be analysed to determine the password. The basic idea of the invention (see paragraph 16, and Figure 1 and paragraph 25) is to overcome this by encrypting the data with different random key data (PS, typically 8 bytes long). The key data is also encrypted with the password (PW) and stored with the encrypted data. This has the advantage that if the encrypted data is analysed, only the key data, which is different for different stored data, can be determined and not the password itself (see paragraph 17).

2. Various prior art documents disclose this basic idea and the examining division considered D3 to be the closest. D3 discloses distributing, e.g. on CDROM, digital content in a digital package or "cryptolope". Different parts of the document are encrypted with different document keys (key data). The document keys are also encrypted under a master key (password) which is stored with each encrypted data part (see diagram and associated text on page 2).

3. The invention defined in claim 1 differs from this essentially by:

(a) generating key data for each logic sector on the storage medium (typically 2 KB)
(b) generating the key data, encrypting it with the password and writing it to the storage medium in an initialising process when creating the logical format
(c) when writing to the storage medium, judging whether or not the encrypted key data have already been read out, decrypted and stored in memory, and if not, reading the relevant encrypted key data and decoding said encrypted key data with said password
(d) a converse reading process comprising steps analogous to those mentioned for writing in paragraph (c) above.

4. The refused main request only included difference (a), and the examining division considered that it solved the problem of enhancing the data confidentiality. They found the solution obvious in the light of D1, which disclosed at column 5, lines 9 to 13, encrypting different sectors of a hard disk using different encrypting keys. The Board agrees with this finding.

5. Difference (b) results in a storage medium with a set of "pre-encrypted" keys for each sector. In other words, they do not need to be generated before being used to encrypt/decrypt data in writing/reading operations, but merely read from the storage medium and decrypted. Furthermore, difference (c) allows for the possibility that a key has already been used and decrypted so that

it does not need to be decrypted again. The application does not state what the effect of these features is, but it could be considered to speed up accesses to the storage medium because the key data has already been generated in advance and may also have been stored in memory for subsequent use.

6. The Board finds neither the features of the solution nor any suggestion of them in any of the prior art. Firstly, starting from D3, the skilled person would have no incentive to speed up the writing process because D3 is not concerned with repeated reading and writing to a storage medium, nor even explicitly with sectors on a storage medium.

7. Secondly, although D1 also mentions speeding up accesses to a disk by using a "preprocessed" secret key, it is a completely different process. In D1, a function f_a is derived from the secret key "a" that is in turn derived from the user password. This function, with the position of the sector to be accessed as a parameter, generates a pseudorandom bit string, expanded to be the same size as the sector on the storage medium (see column 5, line 61 to column 6, line 47). This bit string is XORed with the data to be accessed and is thus comparable with the "key data" of the invention. However, this data is not stored on the storage medium, and since it is also the same size as the data to be accessed, the Board does not consider that a skilled person would envisage storing it.

8. The Board has also considered D2 (US-A-5 267 313), mentioned by the examining division in its first communication, dated 11 March 2004. D2 also discloses,

at column 4, lines 58 to 66 (albeit with the equations (1) and (2) the wrong way round), encrypting data to be protected (X) with key data (DEX) (which should yield "$E_{DEX(X)}$"), and encrypting the key data with a password (TK) (which should yield "$E_{TK(DEX)}$") and writing it all to a storage medium (floppy disk) according to the general idea of the invention.

9. The question arises whether D2 suggests doing this in an initialisation process as claimed. In this respect, the preceding passages mention a security ID "$E_{TK(OEK)}$". This data is not fully described, but it is apparent in analogy with the above nomenclature that it is formed from some data "OEK", "pre-encrypted" with the password TK. This data is said to be "transferred to the terminal security unit 15 to receive the data encryption key DEX, which is used therein for the intended enciphering" (column 4, lines 54 to 57). The nature and origin of "OEK" are not explained and the question is whether "$E_{TK(OEK)}$" is in fact the pre-encrypted key data of the invention, i.e. "$E_{TK(DEX)}$" in the terminology of D2. Given the other inaccuracies in the document, "$E_{TK(OEK)}$" could be a misprint of "$E_{TK(\underline{D}E\underline{X})}$". However, since the priority document (JP application number 3-273501 corresponding to publication number JP-A-06 102822) also contains the same term at column 4, line 31, the Board concludes that the encrypted data "OEK" is some other data that only has a security function and is not related to the key data DEX. Thus in the Board's view D2 does not disclose or suggest storing "pre-encrypted" key data.

10. Accordingly, in the Board's view claim 1 involves an inventive step (Article 56 EPC 1973). The same applies to corresponding apparatus claim 2.

11. The appellant has abandoned claims to some of the embodiments and the description must be amended accordingly. For example, the subject-matter of claim 1 corresponds to the first embodiment including Figures 2, 3 and 4 and paragraphs 25 and 28 of the application. However, in the second embodiment, described at paragraph 35, different key data (R) appears to be generated each time the data is written, although the embodiment also retains the steps of decrypting the initial encrypted key data (see paragraph 35, steps S31 to S33). The third and fourth embodiments, described at paragraphs 37 and 43, respectively, appear to relate to aspects of the invention no longer covered by the claims. The amendment of the description therefore requires careful preparation and the Board considers that the examination of this is a task for the examining division.

Order

For these reasons it is decided that:

1. The decision under appeal is set aside.

2. The case is remitted to the department of first instance with the order to grant a patent on the basis of claims 1 and 2 filed during the oral proceedings before the Board and a description yet to be adapted.

The Registrar: The Chairman:

T. Buschek S. Steinbrener