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

Datasheet for the decision of 8 December 2014

Case Number:	T 1329/10 - 3.5.06
Application Number:	06100077.4
Publication Number:	1688858
IPC:	G06F21/00, H04L9/08
Language of the proceedings:	EN

Title of invention:
Systems and methods for managing multiple keys for file encryption and decryption

Applicant:
Microsoft Corporation

Headword:
Managing multiple keys/MICROSOFT

Relevant legal provisions:
EPC Art. 123(2), 54(1), 56

Keyword:
Amendments of application - allowable (yes)
Novelty - (yes)
Inventive step - (yes)

Decisions cited:

Catchword:

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

Europäisches Patentamt
European Patent Office
Office européen des brevets

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 1329/10 - 3.5.06

DECISION
# of Technical Board of Appeal 3.5.06
of 8 December 2014

Appellant: Microsoft Corporation
(Applicant) One Microsoft Way
Redmond, WA 98052 (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 30 December 2009 refusing European patent application No. 06100077.4 pursuant to Article 97(2) EPC.**

Composition of the Board:

Chairwoman M.-B. Tardo-Dino
Members: A. Teale
S. Krischer

Summary of Facts and Submissions

I. This is an appeal against the decision, dispatched with reasons on 30 December 2009, by the examining division to refuse European patent application No. 06 100 077.4 on the basis that the subject-matter of claim 1 according to the main and two auxiliary requests did not involve an inventive step, Article 56 EPC, in view of the disclosure of the following document:

D1: WO 02/29577 A2.

In a section entitled "Further Remarks" the decision stated that the subject-matter of claim 1 lacked novelty, Article 54 EPC, in view of D4 and that the claimed subject-matter did not involve an inventive step, Article 56 EPC, in view of D3, these documents being as follows:

D3: US 2004/0151310 A1
D4: EP 0 912 011 A2.

II. A notice of appeal was received on 1 March 2010 in which the appellant requested that the decision be set aside and a patent be granted on the basis of the description, claims and drawings on file. The appellant also made an auxiliary request for oral proceedings. The appeal fee was paid on the same day.

III. With a statement of grounds of appeal, received on 10 May 2010, the appellant filed claims according to a main and first and second auxiliary requests and requested that the decision be set aside and a patent granted on the basis of the claims according to said main and first and second auxiliary requests and the pending description and drawings on file. The appellant also reiterated the auxiliary request for oral proceedings.

IV. The application documents on file are consequently as follows:

Description (all requests):
pages 1 and 4 to 18, as originally filed
pages 2, 2a, 2b and 3, received on 16 July 2007.

Claims (all received with the statement of grounds of appeal and identical to the corresponding requests of the appealed decision):
Main request: 1 to 9.
First auxiliary request: 1 to 9.
Second auxiliary request: 1 to 9.

Drawings (all requests):
Pages 1 to 12, as originally filed.

V. The statement of claims according to the main request comprises three independent claims: claim 1 to a computer-implemented method, claim 8 to a computer readable method referring *inter alia* to claim 1, and claim 9 to a computer comprising means adapted to perform the method of *inter alia* claim 1. Claim 1 reads as follows:

"A computer-implemented method for managing multiple keys for file encryption and decryption, the method comprising: decrypting (1000) a list (610, 700) of previously used keys using a prior current key (59B, 701) with which the list of previously used keys has been previously encrypted; adding (1001) the prior current key to the list of previously used keys; and encrypting (1002) the list of previously used keys containing the added prior current key using a new current key."

Reasons for the Decision

1. The admissibility of the appeal

In view of the facts set out at points I to III above, the appeal fulfills the admissibility requirements under the EPC and is thus admissible.

2. The context of the invention

2.1 The application relates to managing data files, for instance in an encrypted file system (EFS). The data files may be stored on a single device (see figure 1) or on different devices linked by a communications network - see figure 2 (not claimed). Each file has been encrypted using a key provided, for instance, on a smartcard. Smartcards may be replaced over time, meaning that the key they contain changes. The description also mentions the user changing the current key; see paragraph [0049], second sentence.

2.2 The issue arises of how to provide long-term access to files as the current encryption key changes, since each file can only be decrypted using the key with which it was originally encrypted; see figure 5. Long-term file access is achieved by storing a list of the respective previous cryptographic keys, the list itself being encrypted using the current cryptographic key.

2.3 Claim 1 of the main request is directed to the method, shown in figure 10, of adding a new current key to the key list. This involves decrypting the list using the prior current key, adding the new current key to the list and then encrypting the list using the new current key; see paragraphs [0069] to [0072]. Claim 1 of the first auxiliary request is directed to the case shown in figure 7 in which different files have been encrypted with different previous keys; see paragraph [0054]. Claim 1 of the second auxiliary request concerns the case of adding a new current key to the key list and then decrypting a file by retrieving its key from the key list to decrypt the file.

3. The prior art

3.1 Document D1

3.1.1 D1 relates to storing data in a database managed *inter alia* by a security administrator. If a user or the security administrator designates a database column as encrypted (see figure 5 and page 8, line 12, to page 9, line 5) then data is automatically encrypted - in a manner which is transparent to the user - before being stored in that column; see figure 6. If the designated column is already encrypted, then it is decrypted using the "previous key" and re-encrypted using a "new key"; see page 3, lines 17 to 21, and figure 5, steps 510 to 518.

3.1.2 The security administrator stores the encryption keys in a keyfile and may also select the mode of encryption, create the keyfile (see figure 3) and establish how many keys are to be stored in the keyfile; see page 3, lines 9 to 11. The keyfile (figure 1; 120) can be stored as an encrypted file in the database system or at a location separate from it; see page 3, lines 13 to 14. The security administrator also moves an obfuscated (i.e. difficult to read) copy (figure 1; 116) of the keyfile to a volatile memory within a server associated with the database system; see page 3, lines 15 to 16. The security administrator can also cause a specified database column to be decrypted and then re-encrypted using a new key; see page 3, lines 17 to 21.

3.1.3 The encryption function in the database server uses keys from the obfuscated keyfile to encrypt data received from the client for storage by a storing function in a row of the database; see figure 6 and page 9, lines 7 to 18. Correspondingly a retrieving function in the database server retrieves data from a row in the database which, if the request is from an authorized user, is then decrypted using keys from the obfuscated keyfile and passed to the client; see page 6, lines 11 to 15 and 20 to 21, page 9, line 20, to page 10, line 9, and figure 7. Metadata stored in the database (see figure 2; metadata 222) records which columns of the database are encrypted and, if so, the key identifier for the key in the obfuscated keyfile that is used to encrypt data in that column and the encryption mode, such as DES; see page 6, lines 22 to 27.

3.1.4 According to the reasons for the appealed decision, the keyfile (120) stored as an encrypted file in the database system can be regarded as the claimed list of previously used keys, the subject-matter of claim 1 of the main request only differing from the disclosure of D1 in the step in which the key, with which the list of keys had been previously encrypted, called the "prior current key", was also stored in the list of keys.

3.1.5 The appellant has disputed whether D1 discloses a prior current key within the meaning of the claims and pointed out that, although D1 mentions the keyfile being stored as an encrypted file, no details are given of the key used to encrypt the keyfile.

3.1.6 The board takes the view that, although D1 mentions the encryption and decryption of specified columns of the database and of the storage of the keyfile as an encrypted file in the database system, there is no mention of encrypting and decrypting files other than the keyfile or of the same key being used to encrypt a database column and the keylist. Already for this reason, the board accepts the appellant's argument that D1 does not disclose a prior current key within the meaning of the claims. It also follows that the board does not accept the statement in the reasons for the decision that "Since databases are stored as files, D1 teaches file encryption and file decryption. D1 discloses a keyfile in which the keys for encryption and decryption are stored. Therefore the keyfile matches the list of keys of the application". While it is true that D1 discloses a keyfile (120) in which keys for encryption and decryption are stored, D1 does not teach file encryption, in particular encryption of a database as a file. Instead, D1 is concerned with encrypting/decrypting individual columns of a database using corresponding individual keys.

3.1.7 In the board's view, the skilled person reading D1 would understand it to follow directly and unambiguously from the re-encryption of a column of the database, previously encrypted with a previous key, using a new key (see page 3, lines 17 to 21) that the new key must be added to the keyfile. Otherwise that database column could not be subsequently decrypted.

This implies that the keyfile is decrypted in order to add the new key and re-encrypted afterwards. However, as the appellant has argued, there is no disclosure in D1 of the key used to encrypt the keyfile, nor is it directly and unambiguously derivable from D1, that the key used to encrypt the keylist afterwards differs from that with which it was decrypted.

3.1.8 The board finds that D1 discloses the following features set out in claim 1 of the main request: a computer-implemented method for managing multiple keys for encryption and decryption, the method comprising: decrypting a list of previously used keys using a prior current key with which the list of previously used keys has been previously encrypted and adding a key to the list.

Hence the subject-matter of claim 1 differs from the disclosure of D1 in that:

a. said multiple keys are used to encrypt and decrypt files;

b. said added key is said prior current key and

c. encrypting the list of previously used keys containing the added prior current key using a new current key.

The board notes that difference "b" corresponds to the difference feature identified in the reasons for the decision. In view of the additional difference features "a" and "c", the disclosure of D1 is less relevant than stated in the decision for the assessment of inventive step (see below).

3.2 Document D4

3.2.1 According to point 6 in section "IV Further Remarks" of the decision, the claimed subject-matter is known from D4, in particular claim 1 in conjunction with paragraphs 14, 18, 25 and 26. The board does not accept this assessment.

3.2.2 The cited passages of D4 relate to the encryption and decryption of a key to provide a backup in case the user forgets it or is unavailable. The encryption/ decryption occurs in two stages. The key is first encrypted using a key derived from the hash of private information, for example the mother's maiden name, and a symmetric encryption algorithm, such as DES. The result is then encrypted using the public key of a trusted party, for example a certificate authority, and an asymmetric encryption algorithm. The original key can be recovered from the resulting "key recovery file" by two corresponding decryption steps, i.e. asymmetric decryption using the private key of the trusted party, followed by symmetric decryption using the key derived from private information.

3.2.3 Since D4 does not disclose an encrypted list of previously used keys, set out in claim 1 according to the main request, it follows that, contrary to the statement in the decision, the subject-matter of that claim is new, Article 54(1,2) EPC 1973, in view of the disclosure of D4.

3.3 Document D3

3.3.1 According to point 5 in section "IV Further Remarks" of the decision, the claimed subject-matter is not inventive in view of the background art acknowledged in

D3. The board is not convinced by this reasoning (see below).

3.3.2 The invention in D3 relates to preventing a previously authorized user from accessing an encrypted file in a shared file system, also termed user revocation, without having to re-key (i.e. decrypt and then re-encrypt using a new key) the file. The problem is solved by giving an authorized user with the old password a "private share" with which he can generate a new cryptographic key based on an old password, the "private share" and a "rotation catalyst" published on a shared bulletin board.

3.3.3 The "background art" section of D3 mentions in paragraph [0005] "lazy revocation" where files are only re-keyed (making them inaccessible to revoked users) when they are updated. Keys are stored in an encrypted file called a "lockbox". In the event of user revocation all of the lockboxes accessed by the revoked user are marked as dirty and any subsequent update to a dirty file causes the file to be re-keyed. To prevent revoked users from accessing unchanged files, paragraph [0006], right-column, lines 3 to 9, teaches re-encrypting all the lockboxes, this necessitating additional key storage for the new lockbox keys.

3.3.4 Hence D3 discloses an encrypted list of keys. There is however no suggestion that the old lockbox encryption key is added to the contents of the lockbox.

4. Inventive step, Article 56 EPC 1973

4.1 Starting from D1

4.1.1 As set out above, the subject-matter of claim 1 differs from the disclosure of D1 in that:

a. said multiple keys are used to encrypt and decrypt files;

b. said added key is said prior current key and

c. encrypting the list of previously used keys containing the added prior current key using a new current key.

4.1.2 Regarding difference "a", the board can see no obvious problem or solution which would lead the skilled person starting from D1 to use the keys used to encrypt/ decrypt specified columns of the database to also encrypt/decrypt files. The board regards the encryption of files as a technical activity which can contribute to inventive step. In view of difference feature "a", the subject-matter of claim 1 involves an inventive step in view of D1.

4.1.3 Difference features "b" and "c" solve the problem of ensuring that users in possession of the new current key can access files encrypted using previous current keys. For the purposes of this decision there is no need to consider whether these features contribute to inventive step.

4.1.4 It follows that the subject-matter of independent claims 8 and 9, which set out a computer readable medium and a computer, respectively, defined by reference to *inter alia* claim 1, also involves an inventive step in view of D1 for the same reasons.

4.2 Inventive step starting from D3

4.2.1 In the light of the above analysis, the background art acknowledged in D3 discloses the following features of claim 1 of the main request: a computer-implemented method for managing multiple keys for file encryption and decryption, the method comprising decrypting a list (lockbox) of previously used keys using a prior current key with which the list of previously used keys has been previously encrypted and subsequently encrypting the list of previously used keys using a new current key.

4.2.2 Hence the subject-matter of claim 1 differs from the disclosure of D3 in that, before the list is re-encrypted, the prior current key is added to the list of previously used keys.

4.2.3 The board can see no obvious problem or solution which would cause the skilled person starting from D3, before the list is re-encrypted, to add the prior current key to the list of previously used keys, in particular because neither the lockbox nor any of the encrypted files is still encrypted with the prior current key. This difference feature solves the technical problem of allowing file decryption and thus can contribute to inventive step.

4.2.4 Hence the subject-matter of claim 1 of the main request involves an inventive step, Article 56 EPC 1973, in view of D3. It follows that the subject-matter of independent claims 8 and 9, which set out a computer readable medium and a computer, respectively, defined by reference to inter alia claim 1, also involves an inventive step in view of D3 for the same reasons.

5. Remittal, Article 111(1) EPC 1973

Considering the prior art on file, the board finds that the reasons set out in the appealed decision for refusing the main request (identical to the current main request) and also the further objections raised in the "Further Remarks" section of the decision concerning novelty and inventive step do not convincingly prove a lack of inventive step or of novelty. The case is thus remitted to the department of the first instance for further prosecution.

Order

For these reasons it is decided that:

The decision under appeal is set aside.
The case is remitted to the first instance for further prosecution.

The Registrar: The Chairwoman:

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

B. Atienza Vivancos M.-B. Tardo-Dino

Decision electronically authenticated