

Internal distribution code:

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

D E C I S I O N
of 3 February 2005

Case Number: T 0275/01 - 3.4.3

Application Number: 94306218.2

Publication Number: 0640946

IPC: G07F 7/12

Language of the proceedings: EN

Title of invention:

Method and apparatus for verification of classes of documents

Patentee:

PITNEY BOWES, INC.

Opponents:

Francotyp-Postalia Aktiengesellschaft & Co. KG
NEOPOST LTD

Headword:

-

Relevant legal provisions:

EPC Art. 54, 56, 113(1)

Keyword:

"Novelty - main request (no)"

"Inventive step - auxiliary requests (no)"

"Right to be heard - New ground of opposition raised at the oral proceedings before the opposition division"

Decisions cited:

G 0007/95, T 0433/93

Catchword:

-



Case Number: T 0275/01 - 3.4.3

D E C I S I O N
of the Technical Board of Appeal 3.4.3
of 3 February 2005

Appellant: PITNEY BOWES, INC.
(Proprietor of the patent) World Headquarters
One Elmcroft
Stamford
Connecticut 06926-0700 (US)

Representative: Avery, Stephen John
Hoffmann Eitle
Patent- und Rechtsanwälte
Arabellastrasse 4
D-81925 München (DE)

Appellant: NEOPOST LTD
(Opponent 2) South Street
Romford, Essex, RM1 2AR (GB)

Representative: Weinmiller, Jürgen
Lennéstrasse 9
D-82340 Feldafing (DE)

Respondent: Francotyp-Postalia Aktiengesellschaft & Co. KG
(Opponent 1) Triftweg 21-26
D-16547 Birkenwerder (DE)

Representative: Schaumburg, Karl-Heinz
Patentanwälte
Schaumburg, Thoenes, Thurn, Landskron
Postfach 86 07 48
D-81634 München (DE)

Decision under appeal: Interlocutory decision of the Opposition
Division of the European Patent Office posted
15 January 2001 concerning maintenance of
European patent No. 0640946 in amended form.

Composition of the Board:

Chairman: R. K. Shukla
Members: G. L. Eliasson
T. Bokor

Summary of Facts and Submissions

I. Oppositions were filed against European patent No. 0 640 946 by Francotyp-Postalia AG & Co. (Opponent O1) and by Neopost Ltd. (Opponent O2) on the ground of opposition under Article 100(a) EPC.

II. In a decision dated 15 January 2001, the opposition division maintained the patent in suit in amended form. In its decision, the opposition division took, inter alia, the following prior art document into account:

D2: US-A-4 853 961, cited by opponent O1.

III. Opponent O2 lodged an appeal on 6 March 2001 paying the appeal fee the same day. A statement of the grounds was filed on 10 May 2001.

The patent proprietor lodged an appeal on 23 March 2001, paying the appeal fee the same day. A statement of the grounds of appeal was filed on 15 May 2001.

IV. Oral proceedings were held on 3 February 2005 in the absence of respondent opponent O1 who had informed the Board in advance that he would not be attending the oral proceedings. The parties made the following requests:

The patent proprietor (appellant) requested that the decision under appeal be set aside and that the patent be maintained on the basis of one of the following requests:

Main Request:

Maintenance of the patent in the form as granted.

First Auxiliary Request:

The maintenance of the patent in the amended form as maintained by the opposition division with the following exceptions:

Reinstatement of:

Figure 4,
the accompanying description given at column 10, lines 35 to 54 of the B specification, the description at column 5, lines 17 to 20, and claims 10 to 13 and 22 to 25 as originally numbered in the granted patent

Second Auxiliary Request:

The maintenance of the patent as maintained by the opposition division.

Opponent O2 (appellant) requested that the decision under appeal be set aside and that the patent No. 0 640 946 be revoked.

V. Independent claims 1 and 14 as granted and according to the patent proprietor's main request read as follows:

"1. A method for verifying a document belonging to a jth class of documents, said jth class being one of a plurality of classes of documents, each of

said classes corresponding to a class encryption/decryption key pair CE, CD, said document incorporating encrypted information $E_i[M]$ comprising information M derived from said document and encrypted with an encryption key E_i for an encryption/decryption key pair E_i, D_i , and said document further incorporating an encrypted decryption key $CE[D_i]$ comprising decryption key D_i for said key pair E_i, D_i encrypted with encryption key CE; for encryption/decryption key pair CE, CD associated with said jth class, said method comprising the steps of:

- a) providing enabling information for enabling retrieval of a decryption key from any document in a selected group of said classes;
- b) determining if said document is in said selected group, and if so retrieving said decryption key D_i from said document;
- c) decrypting said encrypted information $E_i[M]$ to obtain decrypted information $D_i[E_i[M]]$ and deriving said information M from said document; and
- d) comparing said decrypted information $D_i[E_i[M]]$ with said information M to verify the information contained in said document as authentic and unchanged."

"14. An apparatus for verifying a document belonging to a jth class of documents, said jth class being one of a plurality of classes of document, each of said classes corresponding to a class encryption/decryption key pair CE, CD, said document incorporating encrypted information $E_i[M]$ comprising information M derived from said

document and encrypted with an encryption key E_i for an encryption/decryption key pair E_i, D_i , and said document further incorporating an encrypted decryption key $CE_j[D_i]$ comprising decryption key D_i for said key pair E_i, D_i encrypted with encryption key CE_j ; for class encryption/decryption key pair CE_j, CD_j associated with said j th class, comprising:

- a) means (52) for scanning said document (C) to input scanned information, said scanned information including said encrypted information $E_i[M]$, said encrypted decryption key $CE_j[D_i]$, and information identifying said j th class C_j ;
- b) means (58) responsive to enabling information for enabling retrieval of a decryption key from any document in a selected group of said classes of documents and responsive said identifying information C_j to determine if said document is in said selected group, and if so retrieving said decryption key D_i from said scanned information;
- c) means (58) for decrypting said encrypted information $E_i[M]$ from said scanned information to obtain decrypted information $D_i[E_i[M]]$; and
- d) means (62) for comparing said decrypted information $D_i[E_i[M]]$ with said information M to verify the information contained in said document as authentic and unchanged."

VI. Independent claims 1 and 10 as maintained in the decision under appeal and according to the patent proprietor's first auxiliary request read as follows:

- "1. A method for verifying a document belonging to any one of a plurality of classes of documents forming a selected group and corresponding to a plurality of class encryption/decryption key pairs CE, CD, said document incorporating information identifying one class and encrypted information $E_i[M]$ comprising information M derived from said document and encrypted with an encryption key E_i for an encryption/decryption key pair E_i, D_i , and said document further incorporating an encrypted decryption key $CE[D_i]$ comprising decryption key D_i for said key pair E_i, D_i encrypted with encryption key CE; for encryption/decryption key pair CE, CD associated with one relevant class, said method comprising the steps of:
- a) providing a plurality of class decryption keys CD for enabling retrieval of a decryption key D_i from any document in said selected group of said classes;
 - b) reading said class information to determine if said document is in said selected group, and if so retrieving said decryption key D_i from said document by decrypting said decryption key D_i using decryption key CD;
 - c) decrypting said encrypted information $E_i[M]$ to obtain decrypted information $D_i[E_i[M]]$ and deriving said information M from said document; and

- d) comparing said decrypted information $D_i[E_i[M]]$ with said information M to verify the information contained in said document as authentic and unchanged."

"10. An apparatus for verifying a document belonging to any one of a plurality of classes of document forming a selected group and corresponding to a plurality of class encryption/decryption key pairs CE, CD, said document incorporating information identifying one class and encrypted information $E_i[M]$ comprising information M derived from said document and encrypted with an encryption key E_i for an encryption/decryption key pair E_i, D_i , and said document further incorporating an encrypted decryption key $CE_j[D_i]$ comprising decryption key D_i for said key pair E_i, D_i encrypted with encryption key CE; for class encryption/decryption key pair CE_j, CD_j associated with the relevant class, comprising:

- a) means (52) for scanning said document (C) to input scanned information, said scanned information including said encrypted information $E_i[M]$, said encrypted decryption key $CE_j[D_i]$, and information identifying said jth class C_j ;
- b) means (59) storing a plurality of class decryption keys CD_j and means (58) responsive to a relevant class decryption key for enabling retrieval of a decryption key from any document in said selected group of said classes of documents and responsive

said identifying information C_j to determine if said document is in said selected group, and if so retrieving said decryption key D_i from said scanned information;

- c) means (58) for decrypting said encrypted information $E_i[M]$ from said scanned information to obtain decrypted information $D_i[E_i[M]]$; and
- d) means (62) for comparing said decrypted information $D_i[E_i[M]]$ with said information M to verify the information contained in said document as authentic and unchanged."

VII. Independent claims 1 and 14 according to the patent proprietor's second auxiliary request have the same wording as claims 1 and 10, respectively, according to the first auxiliary request.

VIII. The reasons given in the decision under appeal can be summarized as follows:

- (a) The method steps a) to d) in claim 1 as granted includes the case where a single decryption key allows verification of only one class of documents. Consequently, the subject matter of claim 1 as granted is not new having regard to document D2.
- (b) Having regard to document D2, the invention according to claim 1 of the auxiliary request addresses the problem of validating documents reliably from a number of different classes at a single location.

Although document D2 mentions that decryption keys could be geographically dependent, there is no disclosure in document D2 that any of the authorities maintain a database of geographically dependent keys (cf. D2, column 6, lines 11 to 18). Document D2 does not actually deal with verifying different classes of documents at a single location, but teaches that an authority checks only its own documents. Thus, there is no incitement to adapt the teaching of document D2 to a method in which a second authority checks documents of a first authority. As none of the other cited documents suggests different pairs of keys for different classes of documents or the encryption of the decryption key with the document, the subject matter of claim 1 according to the auxiliary request involves an inventive step.

IX. The appealing patent proprietor provided essentially the following arguments in support of his requests:

- (a) The only ground raised by both opponents in their respective notice of opposition was lack of inventive step. An objection of lack of novelty was first raised at the oral proceedings before the opposition division against claim 1 as granted. This constituted a fresh ground of opposition (cf. G 7/95). Following T 433/93, if an opposition division decides to introduce a new ground of opposition, this should be done **in writing** as early as possible, even when the fresh ground is raised during oral proceedings. This procedure was not adhered to, however.

In view of the extremely late introduction of the new ground of opposition, the proprietor did not, at the time of the oral proceedings, have sufficient time within which to consider properly the facts, evidence and arguments. As a result, amendments were made to the patent as granted in a manner not warranted by the true content of document D2.

- (b) Claim 1 according to the main request defines "a document belonging to a j th class of documents, said j th class being one of a plurality of classes of documents, each of said classes corresponding to a class encryption/decryption key pair CE, CD". This feature thus requires that the method should be suitable for carrying verification of any document belonging to any one of the classes of documents. In contrast, the method of document D2 only uses a single class encryption/decryption key pair. Therefore, the subject matter of claim 1 as granted is new.
- (c) The claimed method is furthermore not obvious having regard to document D2. The passages at column 6, lines 11 to 16 of document D2 merely suggests that the method of document D2 could be used separately in a number of different geographical locations. Since document D2 is exclusively concerned with checking mail, document D2 does not give any hint as to how to construct a method which would be suitable for verifying documents belonging to different classes of documents at a single location, where each of the

classes correspond to a different encryption/decryption key pair. On the contrary, it is doubtful whether the authors of document D2 considered the method described therein to be suitable for such applications.

- X. The opponent O2 (appellant) provided essentially the following arguments:
- (a) Regarding the patent proprietor's main request, document D2 envisages that several key pairs can be used (cf. column 6, lines 13 to 16), where each key pair is valid in a separate geographical zone. Therefore, the method of document D2 is able to verify a document belonging to one among several classes of documents where each class is associated with a separate class decryption/encryption key pair. Thus, the method of document D2 has all the features of claim 1 as granted.
 - (b) As to the auxiliary requests, document D2 discloses the possibility of having different geographical zones with different encryption/decryption key pairs (cf. column 6, lines 13 to 16). The problem addressed by the patent in suit, to check documents belonging to different classes of documents at a single site, would for example arise when identification cards are to be checked at a border-crossing using the method of document D2, where each state uses its own class encryption/decryption key pair. Once the skilled person is faced with the problem stated in the patent in suit, he would as a matter of

routine acquire all necessary class decryption keys and store them in the document verification machine.

Reasons for the Decision

1. Both appeals comply with Articles 106 to 108 and Rule 64 EPC and are therefore admissible.
2. *Procedural violation*

The patent proprietor has alleged that due to the introduction of a new ground of the opposition during the oral proceedings, namely, lack of novelty with respect to document D2, he did not have sufficient time to consider properly the new facts, evidence and arguments raised by both the opponents in support of the new ground. Consequently, amendments were made to the patent as granted in a manner which was not warranted by the true content of document D2.

- 2.1 The Board notes that there is no allegation by the patent proprietor that the issue of the decision did not comply with the requirement of Article 113(1) EPC. In the following, however, the Board has considered of its own motion whether or not the patent proprietor's right to be heard was respected before the issue of an adverse decision.
- 2.2 In the present case, the new ground of opposition, i.e. lack of novelty, arose due to an interpretation of claim 1 as granted during the oral proceedings. There was no new prior art introduced in the consideration of

novelty so that no new facts but only new arguments were introduced at the oral proceedings. The Board also notes that the patent proprietor has not alleged that he was not given an opportunity to make submissions on the new interpretation of the wording of claim 1.

2.3 For the above reasons, the Board is of the opinion that the patent proprietor's rights to be heard under Article 113(1) EPC were not violated.

3. *Novelty - Main Request*

3.1 It is common ground that document D2 represents the closest prior art. It discloses a method of authenticating documents sent to an authentication service (cf. abstract; column 4, line 64 to column 5, line 32). The method relies on cipher systems, such as public-key systems, where the encryption key E is different from the corresponding decryption key D, and where it is practically infeasible to compute the decryption key D from knowing the encryption key E. The method disclosed in document D2 is in particular used for checking whether postage printed on mail with a postage meter has actually been paid for.

In the method of document D2, the senders are provided with a class encryption key CE, where the corresponding class decryption key CD is only available to the authentication service. The class encryption key may be the same for all senders, or it could be, for example, geographically dependent, so that all senders throughout a particular geographical region have the same class encryption key CE (cf. column 6, lines 10 to 16).

The sender encrypts information M taken from the document using a document encryption key E_i which is available only to the sender. The corresponding decryption key D_i is encrypted using the class encryption key CE . After that the encrypted information $E_i[M]$ and the encrypted decryption key $CE[D_i]$ are attached to the document, the document is sent to the authentication service, where the class decryption key CD is used to retrieve the decryption key D_i . The encrypted portion M is decrypted using the key D_i , that is, the decrypted information $D_i[E_i[M]]$ is obtained. The decrypted information $D_i[E_i[M]]$ can then be compared with the corresponding plaintext information M from the document.

3.2 The only point in dispute is whether or not document D2 discloses step a) of the method of claim 1. In this connection, the patent proprietor argued that it follows from a purposive interpretation of the preamble of claim 1 that the claimed method of claim 1 requires a plurality of classes j with corresponding class encryption/decryption keys CE_j/CD_j , and that any document belonging to any class j could be verified. Document D2, on the other hand, is concerned with checking mail, and therefore, each post office only has to check mail originating from its own geographical region (cf. item IX(b) above).

3.2.1 The Board agrees however with the decision under appeal that the method of document D2 falls within the scope of claim 1 according to the main request (cf. item VIII(a) above). Step a) of claim 1 only specifies that the decryption key of any document belonging to a

"selected group of said classes can be retrieved". Such a "selected group of said classes", i.e. a subset of all the classes of documents, could consist of only one class, in which case the authorization service would only be able to verify documents belonging to a single class.

Contrary to the patent proprietor's submissions, the Board finds that the above interpretation of claim 1 is purposive in the sense that the construction of the term "group of classes of documents" to encompass a single class is supported by the patent specification: In connection with an embodiment of checking driver's licenses using the claimed method, it is stated in the patent in suit that such an apparatus for validating driver's licenses typically would only be able to validate driver's licenses from the state where the apparatus is located, i.e. the apparatus would contain one class encryption key (cf. patent specification, paragraph [0043]). The apparatus could at a later time be modified for verifying driver's licenses from neighbouring states as well by adding further class encryption keys to the memory of the apparatus (cf. paragraph [0044]).

3.3 For the above reasons, document D2 discloses step a) of claim 1 according to the main request, and therefore, the subject matter of claim 1 according to the main request is not new.

4. *Inventive step - First and Second Auxiliary requests*

4.1 With respect to the main request, the method of claim 1 according to the first auxiliary request further

- specifies that the document to be verified can belong to any one of a plurality of classes of documents, and that a plurality of class decryption keys CD are provided for retrieving the decryption key D_i from the document.
- 4.2 As mentioned above, although document D2 mentions the possibility of having different classes of documents, each with a different class encryption/decryption key pair, this possibility was mentioned in the context of checking mail. Therefore, each authorizing service only checks one class of documents and consequently has access to only one class decryption key.
- 4.3 With respect to the method of document D2, the technical problem to be solved by the patent in suit relates to validating documents reliably from a number of different classes at a single location (cf. patent specification, paragraph [0014]).
- 4.4 The Board agrees with opponent O2 that a skilled person faced with the problem of validating documents from different classes would as a matter of course seek to obtain all class decryption keys for the classes of documents which are to be validated. Since each class decryption key only requires a limited amount of storage space on a computer memory, the verification apparatus could readily be modified to keep all the required class decryption keys in a non-volatile memory.
- 4.5 Although document D2 is mainly concerned with the problem of checking mail, as pointed out by the patent proprietor (cf. item IX(c) above), the disclosure of document D2 relates to document authentication systems

in general (cf. column 1, lines 6 to 10), where a large number of documents have to be authenticated (cf. column 4, lines 20 to 41). Document D2 furthermore discloses how the documents may be divided in different classes of documents, each having a corresponding class encryption/decryption key pair, thereby restricting the authority of the authentication services to check only documents which belong to their assigned class of documents (cf. column 6, lines 13 to 16). Therefore, as the opponent O2 convincingly pointed out, when applying the method of document D2 for checking e.g. identification documents, the need would arise for allowing some authentication services to check documents belonging to more than one class of documents, that is, the need for extending the authority of some authentication services to check documents belonging to more than one class of documents. As stated above under item 4.4 above, however, once the skilled person encounters this problem, he would arrive at the claimed solution in a routine manner.

- 4.6 Since claim 1 according to the second auxiliary request has the same wording as that of the first auxiliary request, the above reasons apply for claim 1 according to the second auxiliary request as well.
- 4.7 For the above reasons, the subject matter of claim 1 according to the first and second auxiliary requests does not involve an inventive step.

Order

For these reasons it is decided that:

1. The decision under appeal is set aside.
2. The European patent is revoked.

The Registrar:

The Chairman:

P. Cremona

R. K. Shukla