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 26 May 2009

Case Number: T 1273/06 - 3.5.02

Application Number: 99123106.9

Publication Number: 1017020

IPC: G07B 17/02

Language of the proceedings: EN

Title of invention:
Controlled acceptance mail fraud detection system

Applicant:
PITNEY BOWES INC.

Opponent:
-

Headword:
-

Relevant legal provisions:
EPC Art. 56

Relevant legal provisions (EPC 1973):
-

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 1273/06 - 3.5.02

D E C I S I O N
of the Technical Board of Appeal 3.5.02
of 26 May 2009

Appellant: PITNEY BOWES INC.
World Headquarters
One Elmcroft Road
Stamford, CT 06926-0700 (US)

Representative: HOFFMANN EITLE
Patent- und Rechtsanwälte
Arabellastrasse 4
D-81925 München (DE)

Decision under appeal: **Decision of the Examining Division of the European Patent Office posted 13 April 2006 refusing European application No. 99123106.9 pursuant to Article 97(1) EPC 1973.**

Composition of the Board:

Chairman: M. Ruggiu
Members: R. Lord
P. Mühlens

Summary of Facts and Submissions

I. This is an appeal of the applicant against the decision of the examining division to refuse European patent application No. 99 123 106.9.

II. In the contested decision the examining division found *inter alia* that the subject-matter of the claims of the main request did not involve an inventive step, thus not meeting the requirements of Article 52(1) EPC in combination with Article 56 EPC. In this respect the following documents of the state of the art were cited:
D1: US-A-5 826 247;
D2: US-A-5 712 787; and
D4: EP-A-0 331 352.

III. In a communication dated 17 February 2009 the board referred also to the following document:
D5: US-A-5 675 650.

IV. The appellant requests that the decision under appeal be set aside and the patent be granted in the following version:

Description
Pages 2, 6, 8 and 9 as originally filed,
Page 5 filed with a letter of 30 November 2004,
Pages 1 and 1a filed with a letter of 16 March 2009,
Pages 3, 3a, 4 and 7 filed with a letter of 02 April 2009.

Claims
Nos. 2 to 7 filed with the letter of 16 March 2009,
No. 1 filed with the letter of 02 April 2009.

Drawings

Sheets 1/3 and 2/3 as filed with a letter of 19 January 2000,

Sheet 3/3 filed with a letter of 30 April 2004.

V. Claim 1 reads as follows:

"A method for processing controlled acceptance mail comprising the steps of:

creating, at a first location, a batch of mail (B) from a plurality of mailpieces (119), each of the plurality of mailpieces having unique indicia data (120) printed thereon which identifies a source (100) of creation of the batch of mail and includes a unique identifier (158) for the mailpiece and a respective validation code (160);

generating, at the first location, a manifest (136) containing all of the unique indicia data (120) for each of the plurality of mailpieces;

sending the manifest (136) to a second location (140);

verifying the authenticity of the manifest at the second location (140);

providing the batch of mail (B) to a carrier distribution system (124) for distribution;

as part of the processing performed by the carrier distribution system (124) reading the unique indicia data (120) from selected mailpieces being distributed therein and sending the unique indicia data for each of the selected mailpieces to the second location (140); and

comparing, at the second location (140), the unique indicia data (120) received from the carrier distribution system (124) for each of the selected

mailpieces with all of the unique indicia data in the manifest (136) to determine if any one of the unique indicia data received from the carrier distribution system matches any one of the unique indicia data in the manifest;
characterized by:
randomly generating a validation code (160) for each of said plurality of mailpieces at the first location;
said indicia data not being cryptographically protected; and
cryptographically protecting the manifest (136) before it is sent to said second location (140)."

Claims 2 to 7 are dependent on claim 1.

VI. The appellant essentially argued as follows:

Claim 1 concerns a method for processing controlled acceptance mail in which, in contrast to the known methods, the indicia data printed on the mailpieces (digital postmark) is not cryptographically protected, and the cryptographic protection is shifted to a manifest containing all of the indicia data, the protection of the printed indicia data being achieved by the provision of a randomly generated validation code for each mailpiece. The provision of the indicia data in a manner which is not cryptographically protected results in the automatic scanning and reading of these data being more reliable. None of the documents on file suggest this shift of the cryptographic protection from the indicia data to a manifest.

Reasons for the Decision

1. The appeal is admissible.

2. *Amendments*

In substance the present claim 1 is equivalent to the combination of claims 1, 4 and 8 as originally filed, which combination was covered by the dependency of those claims.

Additionally the claim has been clarified as follows:

(a) the phrase "*the processing performed by*" has been introduced before the second reference to the carrier distribution system in order to clarify that this system is a physical entity, not a method. This is implicit from the other references in the claim to that system;

(b) the expression "*generating a random validation code*" (in original claim 4) has been amended to "*randomly generating a validation code*", in order to clarify that the generating step, and not merely the resultant code, is random. This clarification has a basis in paragraph [0017], column 5, lines 21 to 27, of the published application; and

(c) the ambiguous expression "*is non-cryptographically protected*" (in original claim 8) has been amended to "*not being cryptographically protected*" so as to exclude the alternative interpretation that the indicia data is protected in a manner which is non-cryptographic. This interpretation, as defined in the amended claim, is the only one which is consistent with the description of the significance of this feature in paragraph [0024]

of the published application.

The remaining amendments to claim 1 are merely formal or linguistic.

Other than the consequential deletion of original claims 4 and 8 the only amendments to the dependent claims are the insertion of a new claim 4, which has a basis in paragraph [0016], column 5, lines 3 to 5 and Fig. 1 of the published application, and the deletion of the second independent claim.

The description of the application has only been amended to be consistent with the claims and to acknowledge the background art disclosed in document D2.

Thus, the amendments to the application meet the requirements of Article 123(2) EPC.

3. *Inventive step*

The document D2 describes (see column 1, lines 53 to 67) a process which allows a postage service provider (CPC) to "*determine and verify postage on automated processing lines*" and uses a barcode printed by the mailer to "*determine factors such as required services and billing information*", and thus concerns a method for processing controlled acceptance mail within the meaning of the present application.

3.1 The method of D2 comprises the following features of the present independent claim 1:

A method for processing controlled acceptance mail

comprising the steps of:

– creating, at a first location ("Customer", see Fig. 1), a batch of mail from a plurality of mailpieces, each of the plurality of mailpieces having unique indicia data printed thereon ("barcode identifier" 1b, column 2, lines 15 to 18) which identifies a source of creation of the batch of mail (Fig. 2, item 2c "Originator", see column 2, lines 29 to 31) and includes a unique identifier for the mailpiece ("Serial Number", also part of item 2c, "*data elements that uniquely identify the mail piece*", column 2, line 30) and a respective validation code (item 2d, "*Security code that functions as an admission password*", column 2, lines 31 and 32);

– generating, at the first location, a manifest containing all of the unique indicia data for each of the plurality of mailpieces ("*electronic manifest*" 1k, the contents of which are described in column 3, lines 35 to 37 and 45 to 52);

– sending the manifest to a second location ("*the EPC 1a automatically creates an electronic manifest 1k to the CPC Customer Server 1e*", column 3, lines 33 and 34 and Fig. 1, noting that from column 3, lines 52 and 53 it is clear that "creates" means "creates and sends", and that the label "Canada Post" in Fig. 1 clearly indicates a different location from "Customer")

– verifying the authenticity of the manifest at the second location ("*CPC Customer Server 1e automatically authenticates the transmission source and verifies the Security Code*", column 3, lines 42 to 44);

– providing the batch of mail to a carrier distribution system for distribution (see Fig. 1,

items 1g and 1n, "Delivery");

– as part of the processing performed by the carrier distribution system, reading the unique indicia data from selected mailpieces being distributed therein ("*the data elements in the barcode identifier 1b are captured by CPC Barcode Sorting Machine 1g*", column 4, lines 18 to 20) and sending the unique indicia data for each of the selected mailpieces to the second location (to the "*data reconciliation application 1h in CPC computing environment*", column 4, lines 29 and 30, noting that it is implicit that the "Customer Server" and the "Data Reconciliation" items both form part of this "environment"); and

– comparing, at the second location, the unique indicia data received from the carrier distribution system for each of the selected mailpieces with all of the unique indicia data in the manifest to determine if any one of the unique indicia data received from the carrier distribution system matches any one of the unique indicia data in the manifest ("*Second level verification is done at the piece level using the Serial Number 2d* [sic] *and other data elements in the identifier ... against the electronic manifest 1m* [sic]", column 4, lines 42 to 46).

3.2 The method of claim 1 is thus distinguished from that of D2 by the following features:

(a) randomly generating a validation code for each of said plurality of mailpieces, whereas in D2, as described in column 2, lines 33 to 35, the "Security Code" is generated by an encryption process, and since it is generated from "[Originator, Date and User Password]", it is

inherently generated only once per day, not once for each mailpiece;

(b) the indicia data not being cryptographically protected, whereas the encryption process of D2 referred to in the previous paragraph implies at least an element of cryptographic protection, even though not all of the indicia data are encrypted; and

(c) cryptographically protecting the manifest before it is sent to the second location, whereas D2 only mentions transmission in a "*secure manner*" (column 3, lines 40 and 41), without indicating what form of security is used.

3.3 Of the above listed distinguishing features, feature (c) considered in isolation would be obvious to the skilled person, since cryptographic protection is a conventional manner of implementing the type of secure transmission already suggested in D2. That this is known in the context of controlled acceptance mail systems is demonstrated by D1, which describes in column 7, lines 42 to 50 that the statement of mail (a document containing information about the batch) is encrypted before being sent from the "mailer" to the "transaction processing center" (i.e. from the first location to the second location in the terminology of the present claim).

3.4 Concerning the above features (a) and (b), it is noted that it is also known to the skilled person to provide an individual validation code for each mailpiece in controlled acceptance mail systems. The most pertinent

example of this knowledge is the document D4, which describes (see column 2, lines 8 to 19) a method in which, as part of the indicia data for the mail, a different pseudo-random number is generated for each franking transaction, which transaction can comprise the franking of an individual mail item (see column 4, line 56 to column 5, line 1). Also in D5 an individual digital token is generated for each mailpiece (see column 5, lines 1 to 29 and column 6, lines 17 to 33). However, the cited passages in both of these documents describe that the validation code (i.e. the pseudo-random number in D4 or the digital token in D5) is encrypted before being incorporated in the indicia data printed on the mailpiece. Moreover neither of these documents describes the creation and transmission of a manifest including all of the indicia data, since D4 does not disclose any such record, and D5 discloses only a "mail documentation file", as depicted in Fig. 7, which does not contain the identifiers of the individual mailpieces, and thus does not constitute a manifest as defined in the present claim 1, but instead corresponds more closely to the "statement of mailing" of the present application.

3.5 Thus D4 and D5 suggest that if individual validation codes are to be generated (for instance randomly, as disclosed in D4), then this development should be combined with encryption of the individual indicia for each mailpiece in order to ensure security. As described in the present application (see paragraph [0024] of the published application, which refers in particular to D5), this has the disadvantages of reduced reliability of the scanning and reading of the indicia and of increased processing time. The technical

problem addressed by the method according to the present claim 1 can be thus seen in providing the increased security associated with individual validation codes whilst avoiding these disadvantages. According to the claim the solution is to modify the method using a manifest, as known from D2, by incorporating individual, randomly generated, validation codes into the indicia data, but to omit the step of encryption of the individual indicia data, the security then being ensured by encrypting the manifest instead. Thus the indicia data printed on the mailpieces are not encrypted, so can be scanned and read more reliably, and only one encryption step is required per mail batch, rather then one per mailpiece, thus reducing the processing time required.

Furthermore, the cryptographically protected manifest can be easily sent to the second location in a manner ensuring its integrity (e.g. electronically, as defined in claim 5), so that the information it contains can be reliably read.

3.6 The prior art documents on file provide no suggestion of this combination of features or the resultant advantages. In particular they provide no suggestion that, if on the basis of D4 and/or D5, individual validation codes were to be introduced into the method of D2, the encryption for each individual mailpiece described in D4 and D5 could be omitted if instead the manifest described in D2 were encrypted. The obvious combination of D2 with D4 and/or D5 would therefore result in a method in which the individual validation codes are cryptographically protected, so that it would not solve the technical problem addressed by the

present application, and would not fall within the terms of the present claim 1. Thus, the subject-matter of claim 1 is considered as involving an inventive step in the sense of Article 56 EPC.

4. The subject-matter of claims 2 to 7, which are dependent on claim 1, is thereby also to be considered as being new and involving an inventive step.

Order

For these reasons it is decided that:

1. The decision under appeal is set aside.

2. The case is remitted to the first instance with the order to grant a patent in the following version:

Description

Pages 2, 6, 8 and 9 as originally filed,
Page 5 filed with a letter of 30 November 2004,
Pages 1 and 1a filed with a letter of 16 March 2009,
Pages 3, 3a, 4 and 7 filed with a letter of 02 April 2009.

Claims

Nos. 2 to 7 filed with the letter of 16 March 2009,
No. 1 filed with the letter of 02 April 2009.

Drawings

Sheets 1/3 and 2/3 as filed with a letter of 19 January 2000,
Sheet 3/3 filed with a letter of 30 April 2004.

The Registrar: The Chairman:

U. Bultmann M. Ruggiu