Internal distribution code:

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

Datasheet for the decision of 27 November 2014

Case Number: T 1226/10 - 3.5.02

Application Number: 04014779.5

Publication Number: 1492055

IPC: G07B17/00

Language of the proceedings: EN

Title of invention:
Method and system for tamper detection

Applicant:
Pitney Bowes Inc.

Relevant legal provisions:
EPC Art. 54, 56

Keyword:
Novelty - (yes)
Inventive step - obvious solution

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 1226/10 - 3.5.02

D E C I S I O N
of Technical Board of Appeal 3.5.02
of 27 November 2014

Appellant: (Applicant)	Pitney Bowes Inc. One Elmcroft Road Stamford, CT 06926-0700 (US)
Representative:	Hoffmann Eitle Patent- und Rechtsanwälte PartmbB Arabellastraße 30 81925 München (DE)
Decision under appeal:	**Decision of the Examining Division of the European Patent Office posted on 15 February 2010 refusing European patent application No. 04014779.5 pursuant to Article 97(2) EPC.**

Composition of the Board:

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

Summary of Facts and Submissions

I. The applicant appealed against the decision of the examining division, posted on 15 February 2010, to refuse the European patent application No. 04014779.5. The statement setting out the grounds of appeal was received on 12 May 2010. With the statement of grounds of appeal the appellant filed anew the set of claims 1 to 12 which had been the subject of the refusal.

II. The examining division held that the subject-matter of claim 1 lacked an inventive step (Article 56 EPC) in the light of document:

D1 = "Information Based Indicia Program Postal Security Device Specification", United States Postal Service, 13 June 1996, pages i to A-1, XP002137734.

III. In an annex to the summons to oral proceedings dated 21 July 2014 the Board expressed its preliminary opinion that the subject-matter of claim 1 did not appear to involve an inventive step in the light of the combination of document D1 with document US 6 230 149 B1 (D4), introduced by the Board and showing that the problem addressed by the application was known.

IV. Oral proceedings before the Board took place as scheduled on 27 November 2014.

V. The appellant requested that the decision under appeal be set aside and that a patent be granted on the basis of the set of claims 1 to 12 filed with letter dated 11 May 2010.

VI. Claim 1 of the appellant's current request reads as follows:

"A method for a data center (40) to process usage data of a value dispensing device (12) comprising:

receiving (52) a first audit record from the value dispensing device (12), the first audit record generated by the value dispensing device (12) at a start of an audit period, the first audit record including a value of at least one register maintained by the value dispensing device at the start of the audit period, a time stamp, and a first digital signature;

receiving (60) a second audit record from the value dispensing device (12), the second audit record generated by the value dispensing device (12) at an end of the audit period, the second audit record including a value of the at least one register maintained by the value dispensing device at the end of the audit period, a time stamp, and a second digital signature;

receiving (62) usage data from the value dispensing device (12) for the audit period;

verifying (82) the first and second digital signatures;

verifying (88) the time stamp in the first audit record corresponds to the start of the audit period and the time stamp in the second audit record corresponds to the end of the audit period;

if the first and second digital signatures verify and the time stamp in the first audit record corresponds to the start of the audit period and the time stamp in the

second audit record corresponds to the end of the audit period, determining (94) a difference between the value of the at least one register at the end of the audit period and the start of the audit period;

comparing (96) the determined difference with corresponding data provided in the usage data; and

if the determined difference is the same as the corresponding data provided in the usage data, generating (100) a usage report for the value dispensing device (12) based on the usage data."

VII. The appellant essentially argued as follows:

The United States Postal Service required that the PSD (Postal Security Device) transmits audit messages formatted as shown in table 3.2.5 of D1 to the data center. The values of the ascending and descending registers included in the audit messages were snapshots of the postal security device records. D1 was silent about the use of the audit messages and did not discuss the transmission of any usage data.
D4 was relevant, since it mentioned the usage data and showed what was done at that time to authenticate usage data messages. D4 did not simply address the problem underlying the present invention, namely detecting whether the user data had been tampered with, but proposed a solution and discussed how the data center was involved in that solution. With the solution of D4 a printed document comprising a readable usage data message and an authentication mark produced at the user side (cf. figure 4) was transmitted to the data center. At the data center the authentication mark was decrypted and compared with the readable data printed on the document. The transmission of the document took

place independently of the transmission of the compulsory audit messages by the PSD. In D4 the authentication mark and the readable message were both established at the user side and could therefore have easily been tampered with.
Finally a similar method was disclosed in D3 (GB 2 293 737 A).
The invention had the advantages that it reduced the amount of data transmitted from the PSD, and that it reduced the amount of data which had to be encrypted there.
The method of claim 1 also raised the degree of assurance that the usage data was accurate and not tampered with before the report was generated by transmitting solely the usage data and making use of the PSD secure records.

Reasons for the Decision

1. The appeal is admissible.

2. Novelty

2.1 It is not disputed that the document D1 represents the most relevant prior art. D1 discloses a method for a data center (USPS IBIP infrastructure) to process data of a value dispensing device (PSD), which comprises receiving audit records from the value dispensing device, the audit record including a value of at least one register maintained by the value dispensing device, a time stamp and a digital signature (cf. page 3-19, paragraph 3.2.4, page 3-21, table 3.2.5), whereby two consecutive audit records (messages) may be considered as first and second audit records, and whereby it is implicit that the time stamps and digital signatures

included in these messages are verified at the data center (cf. item 2.1.1. of the reasons for the decision under appeal).

2.2 The method according to claim 1 is new having regard to D1 (Article 54 EPC) since it differs by:

a) - "receiving (62) usage data from the value dispensing device (12) for the audit period";

b) - "determining (94) a difference between the value of the at least one register at the end of the audit period and the start of the audit period";

c) - "comparing (96) the determined difference with corresponding data provided in the usage data"; and

d) - "if the determined difference is the same as the corresponding data provided in the usage data, generating (100) a usage report for the value dispensing device (12) based on the usage data".

3. Inventive step

3.1 The reception of usage data from each customer is a requirement set by some postal authorities, for use for instance in statistical analysis (see e.g. paragraph [0005] of the published application). This is therefore a non-technical requirement, as argued in the decision under appeal. Since the PSD is de facto in communication with the data center for transmitting messages, it is obvious to use the PSD to transmit the usage data from the customer to the data center. Feature a) above therefore cannot contribute to the presence of an inventive step.

3.2 The ascending and descending registers mentioned in the audit messages defined in table 3.2-5 of D1 contain encrypted values related to the usage of postal

services. These values are foreseen to be used for an audit of the usage of postal services.

3.3 An audit of the usage of postal services inherently consists in estimating a usage over a time span. The values of the ascending and descending registers are snapshot values of the usage of the postal services. It is therefore immediately obvious for a person skilled in the art that only the difference of two snapshot values of the same register, transmitted in two audit records which de facto would represent respectively the start and the end of an audit period, could represent a consumption over a time period, i.e. only the difference of two snapshot values would represent a value comparable with the usage data reported by the customer of the postal services, the comparison itself being necessary to conclude the audit, to assess the validity of the received usage data and to generate the final report.
Hence, starting from D1, the technical aspects of features b), c) and d) represent only straightforward steps of implementing the required procedures at the data center of the postal service.

4. Appellant's counter-arguments

4.1 According to the appellant, the problem to be solved by the method of claim 1 is to raise the degree of assurance "that the usage data is accurate and was not tampered with before the report was generated" (cf. statement of grounds of appeal at page 3, paragraph 2, and sections [0007] and [0008] of the published application).
The usage data, which is defined in section [0005] of the published application, is not securely stored in the postal security device (PSD), also called value

dispensing system, and may thus be modified before being transmitted (cf. section [0006]). The claimed solution involves comparing received usage data with corresponding data encrypted in the compulsory secure audit records.

4.2 The appellant argues that this problem is acknowledged in document D4 (cf. column 1, lines 28 to 32 and 60 to 63) and that the solution described there, which involves the transmission of a document comprising usage data and an encrypted authentication mark produced at the user side and printed on the document (cf. figure 4 and column 3, line 65 to column 5, line 13), would therefore be the obvious solution to that problem. He mentioned also that a similar solution was disclosed in D3. He concluded further that the claimed solution would not be obvious, in particular because of the advantages in terms of reducing the amount of data transmitted to/from the PSD and reducing the demands on the encryption device.

4.3 The board does not find this argument convincing, primarily because D4 merely demonstrates that a different solution to a similar problem was known. This does not alter the fact that, for the reasons discussed in paragraphs 3.1 to 3.3 above, the claimed solution would be obvious from D1 alone. The board notes moreover that, as the appellant himself has pointed out, the problem addressed by D4 is different in detail from that addressed in the present application, since D4 is concerned with authenticating the source of the information, whereas the present application is concerned with the authenticity of the usage data itself. Accordingly, as the appellant has also noted, the method of D4 would not prevent tampering with the usage data between its generation and its encryption at

the user side, so that it would not address the problem of the present application as effectively as the claimed method. The board therefore concludes that the skilled person would not have chosen the solution of D4 in preference to that derived in an obvious manner from D1, but would instead have merely recognised that it shows that the concept of validating usage data by comparing it with secure PSD data was as such known. In this context the teaching of D3 is no more relevant than that of D4.

5. The board therefore concludes that the subject-matter of claim 1 of the appellant's sole request does not involve an inventive step according to Article 56 EPC. Hence the appeal has to be dismissed

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chairman:

U. Bultmann R. Lord

Decision electronically authenticated