Internal distribution code:

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

Datasheet for the decision of 9 December 2015

Case Number: T 2217/11 - 3.4.03

Application Number: 01924079.5

Publication Number: 1386296

IPC: G07F19/00, G06F17/60

Language of the proceedings: EN

Title of invention:
METHOD FOR SECURE PAYMENT WITH MICROPAYMENT CAPABILITIES

Applicant:
milliPay Systems AG

Headword:

Relevant legal provisions:
EPC Art. 52(1), 52(2), 52(3), 123(2)
EPC 1973 Art. 56

Keyword:
Amendments - added subject-matter (no)
Patentable invention - (yes)
Inventive step - (yes)

Decisions cited:
T 0258/03, T 0789/08

Catchword:

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 2217/11 - 3.4.03

D E C I S I O N
of Technical Board of Appeal 3.4.03
of 9 December 2015

Appellant: (Applicant)	milliPay Systems AG Schaffhauserstrasse 560 8052 Zürich (CH)
Representative:	Rentsch Partner AG Rechtsanwälte und Patentanwälte Fraumünsterstrasse 9 Postfach 2441 8022 Zürich (CH)
Decision under appeal:	**Decision of the Examining Division of the European Patent Office posted on 10 June 2011 refusing European patent application No. 01924079.5 pursuant to Article 97(2) EPC.**

Composition of the Board:

Chairman	G. Eliasson
Members:	S. Ward
	C. Heath

Summary of Facts and Submissions

I. The appeal is against the decision of the Examining Division refusing European patent application No. 01 924 079 on the grounds that the claims "relate to subject-matter excluded from patentability under Art. 52(2) and (3) EPC" and that the claimed subject-matter did not involve an inventive step within the meaning of Article 56 EPC.

II. The appellant requested in writing that the decision under appeal be set aside, and that a patent be granted based on:

- Claim 1 as filed with the letter dated 25 November 2015;
- Description: pages 1, 1a, 3-9 filed with the letter dated 19 November 2015; page 2 filed with the letter dated 25 November 2015; and
- Drawings: sheets 1/3 - 3/3 as originally filed.

III. The following document (Reference [1] cited in the application on page 9) is referred to in this decision:

D0: Rivest et al., PayWord and MicroMint: Two Simple Micropayment Schemes; Security Protocols, Proceedings of the International Workshop, Cambridge, UK, April 10-12 1996; Lecture Notes in Computer Science, Springer 1997; pages 69-87.

IV. Claim 1 reads as follows:

"A method for secure payment via a communication network, the method involving in a payment session three agents, a customer (C), a broker (B) and a vendor (V), the method comprising an initialization phase for starting the payment session and propagating shared secret data, and a continuation phase for proceeding the session and propagating payment transaction tokens, the initialization phase comprises:

transmitting from the vendor (V) to the customer (C), responsive to a request from the customer (C), a first message including a certificate C_v of the vendor (V), the first element v_0 of a payment chain v and price information, the payment chain v being a secure chain calculated by the vendor (V) as a secure sequence of integers using a cryptographically strong hash function and a randomly selected first member, and the price information and the first element v_0 being signed by the vendor (V) with a secret key V_{sk} of the vendor (V), verifiably with a corresponding public key V_{pk} of the vendor (V);

transmitting from the customer (C) to the broker (B) a second message including a certificate C_c of the customer (C), the first element c_0 of a customer authorization chain c, the customer authorization chain c being a secure chain calculated by the customer (C) as a secure sequence of integers using a cryptographically strong hash function and a randomly selected first member, and the first message, the first element c_0 and the first message being signed by the customer (C) with a secret key C_{sk}, of the customer (C), verifiably with a corresponding public key C_{pk} of the customer (C); and

transmitting from the broker (B) to the vendor (V) a message including the first element v_0 of the payment chain v, and the first element b_0 of a broker authorization chain b, the broker authorization chain b being a secure chain calculated by the broker (B) as a secure sequence of integers using a cryptographically strong hash function and a randomly selected first member, and the first element v_0 of the payment chain v and the first element b_0 of the broker authorization chain b being signed by the broker (B) with a secret key B_{sk} of the broker (B), verifiably with a corresponding public key B_{pk} of the broker (B);

and wherein the continuation phase comprises:

transmitting from the vendor (V) to the customer (C) a payment request token including an element v_{ni} of the payment chain v, and an index n_i indicating the position of the element v_{ni} in the payment chain v;

transmitting from the customer (C) to the broker (B) a payment order token including the element v_{ni} of the payment chain v and the index n_i received from the vendor (V), and an element c_j of the customer authorization chain C; and

transferring by the broker (B) a payment amount to an account of the vendor (V), responsive to receiving the payment order token from the customer (C), the payment amount being determined by a multiplication of a currency unit with a difference between the index n_i received from the vendor (V) in the payment order token and an index n_{i-1} of an element v_{ni-1} of the payment chain v received previously by the broker (B) from the customer (C),

transmitting from the broker (B) to the vendor (V) a payment confirmation token including the element v_{ni} of the payment chain v and the index n_i received from the customer (C), and an element b_j of the broker authorization chain b; and

the vendor (V) sending data paid by the customer (C), upon receiving the payment confirmation token."

V. The appellant's arguments, insofar as they are relevant to the present decision, may be summarised as follows:

The document D0 was seen as the closest prior art in the contested decision. The "PayWord" method described therein was explicitly stated to be credit-based (page 70, section 3, first line).

According to this method, the broker issued and transmitted to the customer (user) a digitally-signed certificate, which authorized the customer to generate PayWord chains. The customer created the PayWord chain $w_i=h(w_{i+1})$ in reverse order from a randomly selected last payword w_n, and computed and signed a commitment including the root w_0, and provided this commitment to the vendor.

At the end of each day, the vendor reported to the broker the last (highest-indexed) payment (w_L, L) received from the customer that day with each corresponding commitment. Subsequently, the broker charged the customer’s account L cents and payed L cents into the vendor’s account.

PayWord was therefore an *off-line* scheme where the vendor did not need to interact with the broker when the customer (user) first contacted the vendor, nor did the vendor need to interact with the broker as each payment was made. The secure chains were used by the customer to indicate to the vendor a commitment, whereupon the vendor would deliver the ordered goods to the customer.

In such a credit-based scheme, if the customer's account was empty, the vendor might not get paid for the delivered goods.

In contrast, the method claimed in present application was strongly debit oriented, as could be seen from the steps illustrated in Figure 4.

In the claimed method for secure payment, the vendor sent to the customer the paid data only *after* the confirmation from the broker that the payment amount had indeed been transferred from the account of the customer to the account of the vendor.

The claimed method for secure payment not only differed from the PayWord method in that three secure chains were used, but it further differed in that these secure chains were used in different ways (different directions and sequences), making it possible to implement a secure debit-oriented payment method rather than the credit-oriented method of PayWord.

One skilled in the art did not find any reference or motivation in document D0 that would lead to the claimed debit-oriented method for secure payment.

Reasons for the Decision

1. The appeal is admissible.

2. Article 123(2) EPC

2.1 Claim 1 introduces an "initialization phase" and a "continuation phase", and then describes these phases in detail. The initial introduction is based essentially on claim 1 as filed. That the invention relates to communication network payment schemes is clear from the first line of the description. The term "payment session" is defined under the heading "Session" on page 3.

2.2 The features of the initialization phase are present in outline in claim 2 as originally filed (and Figure 1). Several features appeared in original claim 2 only in symbolic form, and the corresponding definitions of these symbols have been imported into the claim. The definition of the data sent among the agents is based on the section "Session initialization scheme" bridging pages 3 and 4, and the details of the secure chains and the cryptographic aspects are based on paragraphs of the "Description of the Invention" on page 2.

2.3 The features of the continuation phase are present in outline in claim 5 as originally filed (and Figure 4). In the present claim, the terms used in original claim 5 have been more fully defined with reference to the section "Scheme 3", bridging pages 5 and 6. In particular, the claimed steps commencing "transmitting from the vendor...", "transmitting from the customer...", and "transmitting from the broker...",

are based on steps 1, 2 and 3 of this section. The claimed step commencing "transferring by the broker ..." is based on the final paragraph on page 5.

2.4 Present claim 1 specifies a "payment request token", a "payment order token" and a "payment confirmation token". Although these terms do not appear expressly in the original application, claim 1 as filed refers to "a cyclic propagation of payment transaction tokens", and since the cycle referred to comprises a request, an order and a confirmation, the Board has no objection to this amendment.

2.5 In relation to the final feature of the claim, the properties of scheme 3 are the same as those of scheme 1, apart from a possible variable price (page 6, lines 4-6), and according to scheme 1: "vendor expects payment confirmation to start sending data paid by the customer".

2.6 The subject-matter of claim 1 therefore meets the requirements of Article 123(2) EPC.

3. Patentability

3.1 The Examining Division found that the claims related to "subject matter excluded from patentability under Art. 52(2) and (3) EPC." No subsection of Article 52(2) EPC was mentioned, but in the light of the comments in the final two paragraphs on page 4 of the Reasons, it would appear that the claimed invention was considered to be a method of doing business, and therefore excluded by Article 52(2)(c) EPC.

3.2 Although methods of doing business are excluded from patentability by Article 52(2)(c) EPC, this is only to

the extent to which the application relates to methods of doing business "as such" (Article 52(3) EPC).

In the present case, claim 1 seeks protection for a method for secure payment via a communication network, and the subject-matter is chiefly defined in terms of a sequence of messages exchanged between three agents, the content of the messages and the extent and nature of the encryption used being set out in detail. The subject-matter of the claim does not, therefore, relate to a method of doing business "as such", but rather to the field of secure communication over a network using cryptography, and hence it has a technical character (see e.g. T 789/08, Reasons, point 3.2, first paragraph).

3.3 The Board accepts that claim 1 comprises certain individual features which might be seen as purely related to business, for example transferring by the broker a payment amount to an account of the vendor. This, however, is irrelevant. By virtue of the technical features referred to above, the claimed method is an invention within the meaning of Article 52(1) EPC and not excluded from patentability under Articles 52(2) and (3) EPC 1973 (see e.g. T 258/03, Points 4.1 to 4.7).

4. Inventive Step

4.1 According to the application (see "Background of the Invention"), the starting point for the present invention is the document D0 ("Rivest et al.", cited as reference [1] in the description), as acknowledged in the contested decision (see point 4.3). In particular, the "PayWord" method disclosed in document D0 (section

3, pages 70-75) has been extensively referred to by the appellant in its submissions on inventive step.

"PayWord" is a known method for secure payment via a communication network, and therefore has the same general purpose as the present invention. Furthermore, the claimed method and PayWord have at least the following features in common: an exchange of data between a customer, a broker and a vendor; a user generated secure chain calculated using a hash function; an initial phase including public key operations, including certification and the sharing of the root of the chain; and the possibility of variable size payments.

The Board is therefore satisfied that the Payword method of document D0 represents a reasonable starting point for the discussion of inventive step.

4.2 The PayWord method is credit-based, in that the user's account is charged by the broker at the end of each day for goods already received. As pointed out by the appellant, this exposes the broker to risk if the customer's account cannot cover the transactions. By contrast, the claimed system is debit-based, with payments being transferred to the account of the vendor and a confirmation sent to the vendor before the goods (data) are sent from the vendor to the customer.

Merely switching from a credit-based method to a debit-based method is clearly not in itself inventive, nor has this been argued by the appellant. In fact, the possibility of operating the PayWord method on a debit basis is foreseen on page 75 of document D0 ("Paywords could be sold on a debit basis, rather than a credit

basis ..."), in which case the broker would need to be involved in each transaction, as in the claimed method.

The appellant argues, however, that the specific features of the claimed method (three secure chains being used according to different directions and sequences compared with PayWord) make it "possible to implement a secure *debit-oriented* payment method rather than the *credit-oriented* method of PayWord."

4.3 Using the symbols employed in the application, the details of the information sent among the agents according to the claimed scheme may be summarised as follows:

Initialisation Phase:
1. C to V: request
2. V to C: C_v,{v_0, price information}V_{sk}
3. C to B: C_c,{c_0, C_v, {v_0, price information}V_{sk}}C_{sk}
4. B to V: {v_0, b_0}B_{sk}

Continuation Phase:
5. V to C: payment request (v_{ni}, n_i)
6. C to B: payment order (v_{ni}, n_i)c_j
7. B to V: payment confirmation (v_{ni}, n_i)b_j

In addition, between messages 6 and 7, B transfers to the account of V a payment amount equal to currency unit * (n_i - n_{i-1}).

4.4 Steps 2-7 are not disclosed in document D0, and the problem solved by these distinguishing features is seen as implementing a secure debit-oriented payment method.

4.5 The claimed method sets out a precise sequence of messages sent between three agents, with the content of each message prescribed in detail, and differing considerably from the corresponding messages of the PayWord method.

For example, in document D0 the initialisation phase comprises a step in which the root element w_0 of a secure chain w is sent from the customer (user) to the vendor. This is the only secure chain used in the PayWord method.

By contrast, in the initialisation phase of the claimed method, the root element v_0 of a secure chain v is sent from the vendor to the customer (hence in the opposite direction to that of document D0), then the root elements c_0, v_0, of **two** secure chains c, v are sent from the customer to the broker (the message also comprising two signatures Vsk, Csk), and finally the root elements v_0, b_0, of **two** secure chains v, b are sent from the broker to the vendor.

In the opinion of the Board, such a modification goes beyond anything which could legitimately be described as a trivial or obvious extension of the PayWord method. The Board has also not found any disclosure or hint in the other available prior art which would lead the skilled person to the present invention.

4.6 The subject-matter of claim 1 is therefore judged to involve an inventive step within the meaning of Article 52(1) EPC and Article 56 EPC 1973.

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 in the following version:

   - Claim 1 as filed with the letter dated 25 November 2015;
   - Description: pages 1, 1a, 3-9 filed with the letter dated 19 November 2015; page 2 filed with the letter dated 25 November 2015; and
   - Drawings: sheets 1/3 - 3/3 as originally filed.

The Registrar: The Chairman:

S. Sánchez Chiquero G. Eliasson

Decision electronically authenticated