

Internal distribution code:

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

**Datasheet for the decision
of 20 July 2021**

Case Number: T 0994/18 - 3.5.01

Application Number: 10833691.8

Publication Number: 2504801

IPC: G06Q20/00, G06Q20/32

Language of the proceedings: EN

Title of invention:

SECURE MOBILE PAYMENT PROCESSING

Applicant:

Advanced New Technologies Co., Ltd.

Headword:

Secure mobile payment/ADVANCED NEW TECHNOLOGIES

Relevant legal provisions:

EPC Art. 123(2), 56

Keyword:

Amendments - added subject-matter (yes)
Inventive step - payment process using a known technical
infrastructure for encrypting data (no - obvious
implementation)



Beschwerdekammern
Boards of Appeal
Chambres de recours

Boards of Appeal of the
European Patent Office
Richard-Reitzner-Allee 8
85540 Haar
GERMANY
Tel. +49 (0)89 2399-0
Fax +49 (0)89 2399-4465

Case Number: T 0994/18 - 3.5.01

D E C I S I O N
of Technical Board of Appeal 3.5.01
of 20 July 2021

Appellant: Advanced New Technologies Co., Ltd.
(Applicant) Cayman Corporate Centre
27 Hospital Road
George Town, Grand Cayman KY1-9008 (KY)

Representative: McKinnon, Alistair James
WP Thompson
138 Fetter Lane
London EC4A 1BT (GB)

Decision under appeal: **Decision of the Examining Division of the
European Patent Office posted on 7 December 2017
refusing European patent application No.
10833691.8 pursuant to Article 97(2) EPC.**

Composition of the Board:

Chairman W. Chandler
Members: R. Moser
C. Schmidt

Summary of Facts and Submissions

- I. This appeal is against the examining division's decision to refuse European patent application No. 10833691.8.
- II. The examining division found that claim 1 of the main and auxiliary request was not inventive over a "distributed networked information system exchanging both encrypted and unencrypted data". They considered that the essential idea of the invention related to a payment, thus, to a business method.
- III. The appellant requested that the decision under appeal be set aside and that a patent be granted on the basis of the main or first auxiliary request filed with the statement setting out the grounds of appeal. The main request essentially corresponded to the refused auxiliary request.
- IV. In the communication accompanying the summons to oral proceedings, the Board expressed its doubts that the auxiliary request met the requirements of Article 123(2) EPC. Furthermore, it considered that none of the requests was inventive over D1.
- V. In a reply, dated 18 June 2021, the appellant replaced the previous requests with a single "MAIN REQUEST" and provided arguments in favour of compliance with Article 123(2) EPC and inventive step.
- VI. With letter dated 19 July 2021 the appellant informed the Board that it would not attend the oral proceedings and requested a decision on the basis of the papers on

file.

VII. Oral proceedings took place in absence of the appellant on 20 July 2021 by videoconference. At the end of the oral proceedings the Chairman announced the Board's decision.

VIII. The appellant's requests are as follows:

- that the decision under appeal be set aside
- that a patent be granted on the basis of the main request filed with the letter dated 18 June 2021.

IX. Claim 1 of the sole request reads:

"A method for processing payment data, comprising:
generating a first payment amount;
transmitting (301) recipient information to a payer terminal (102), wherein the recipient information comprises a recipient account number, the generated first payment amount, and a payment serial number that uniquely identifies a current payment;
receiving (302) a second payment amount and encrypted payment request data returned from the payer terminal (102), wherein a definition of an encryption function is pre-stored in a file accessible by the payer terminal (102) and a payment server (106), wherein the payer terminal (102) encrypts payment request data using a public key of the payment server (106) to obtain the encrypted payment request data, wherein the definition of the encryption function is unknown to a recipient terminal (104), wherein the encrypted payment request data comprises an encrypted third payment amount, an encrypted payer information, and an encrypted recipient information, wherein the second payment amount relates to an unencrypted version of the third payment amount, wherein the payer

information includes a payment account number and a payer password, and wherein the encrypted payment request data is encrypted by an encryption technique that is prearranged between the payer terminal (102) and the payment server (106);

comparing the generated first payment amount with the second payment amount in the event that the second payment amount is not sent by the recipient terminal and is input by the payer terminal; and

in the event that the generated first payment amount matches the second payment amount:

forwarding the encrypted payment request data and a first payment amount to the payment server (106), wherein the payment server, via the definition of the encryption function, is to decrypt the encrypted payment request data to obtain received payer information, compare the received payer information with pre-stored payer information, and in the event that the received payer information matches the pre-stored payer information, send encrypted payment result data;

receiving (303) the encrypted payment result data from the payment server (106), the encrypted payment result data indicating whether a payment is successfully made by the payment server (106), wherein the encrypted payment result data includes a payment time and is encrypted using the encryption technique by the payment server (106); and

returning (304) the encrypted payment result data to the payer terminal (102)."

- X. The appellant argued that claim 1 of the new request no longer contained added subject-matter and was inventive over the prior art.

Reasons for the Decision

1. Claim 1 of the sole request corresponds in substance to claim 1 of the auxiliary request filed with the grounds of appeal.

2. It relates to a secure mobile payment method ([0004]) in which essentially a merchant's POS ("recipient terminal") sends an invoice, including a "first" payment amount, to a customer's mobile phone ("payer terminal"), which returns a "second" payment amount and an encrypted payment request. The second payment amount is either the first payment amount or an amount entered by the customer. The POS cannot decipher the payment request, but can only forward it to a payment server if the second payment amount is equal to the first payment amount.

3. Added subject-matter

- 3.1 The claim still defines that the merchant transmits a first payment amount ("the recipient information **comprises ... the generated first payment amount**", emphasis added by the Board) to and receives a second payment amount from the customer, furthermore, that these amounts are compared before forwarding payment data to the server.

However, as set out in point 6.1 of the Board's communication, this is not disclosed in the description, see for example paragraphs [0032] and [0033], where a comparison is only performed if the merchant does not transmit a first payment amount to the customer.

4. Inventive step

4.1 As set out in more detail in its communication (points 6.6 and 6.7), the Board judges that claim 1 is an obvious implementation of a business method on the technical infrastructure of D1, comprising a stationary terminal relaying encrypted data between a mobile terminal and a server.

4.2 Even taking the appellant's latest arguments into consideration, the Board judges that the decision to include or exclude the payment amount in the information which the merchant provides to the customer is not based on technical considerations. In particular, this is not related in any way to the effects mentioned by the appellant, i.e. reduced data transmission, cryptography or improved security.

Firstly, preventing payment in case of an incorrect amount entered by the customer is a business need - not transmitting payment data to the server follows directly from this need.

Secondly, irrespective of whether or not the customer enters a payment amount he communicates with the merchant and, thus, in this sense is verified.

The Board also notes that the payment amount cannot be equated to a one-time-pad. The latter has a specific technical meaning, namely that of a random secret key for encrypting a plain text, which is not what the payment amount is used for.

Thus, the Board does not see that any of the features relating to which party enters the payment amount, be it the merchant or the customer, is connected to the

security of the system, let alone that it provides an improved security over D1.

5. The Board, thus, concludes that claim 1 is not allowable for added subject-matter (Article 123(2) EPC) and for lack of inventive step (Article 56 EPC).

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar:

The Chairman:



T. Buschek

W. Chandler

Decision electronically authenticated