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

Datasheet for the decision
of 8 July 2010

Case Number: T 0973/07 - 3.4.03

Application Number: 02254285.6

Publication Number: 1271427

IPC: G07F 7/08

Language of the proceedings: EN

Title of invention:
Transaction terminal apparatus

Applicant:
FUJITSU LIMITED

Opponent:
-

Headword:
-

Relevant legal provisions:
-

Relevant legal provisions (EPC 1973):
EPC Art. 56

Keyword:
"Inventive step (yes)"

Decisions cited:
-

Catchword:
-

Case Number: T 0973/07 - 3.4.03

D E C I S I O N
of the Technical Board of Appeal 3.4.03
of 8 July 2010

Appellant:
FUJITSU LIMITED
1-1, Kamikodanaka 4-chome
Nakahara-ku
Kawasaki-shi
Kanagawa 211-8588   (JP)

Representative:
Gibbs, Christopher Stephen
Haseltine Lake LLP
Lincoln House, 5th Floor
300 High Holborn
London WC1V 7JH   (GB)

Decision under appeal:
Decision of the Examining Division of the European Patent Office posted 29 November 2006 refusing European application No. 02254285.6 pursuant to Article 97(1) EPC 1973.

Composition of the Board:

Chairman: G. Eliasson
Members: V. L. P. Frank
                   J. Van Moer

C4138.D

Summary of Facts and Submissions

I.   This is an appeal from the refusal of application
       02 254 285 for the reason that the subject-matter of
       claim 1 did not involve an inventive step (Article 56
       EPC 1973).

II.   At oral proceedings before the board, the appellant
       applicant requested that the decision under appeal be
       set aside and that a patent be granted on the basis of
       the request filed during oral proceedings.

III.   The independent claim of this request reads as follows
       (the difference with respect to the version of the
       claim refused by the examining division was highlighted
       by the board):

       "1. A **portable** transaction terminal apparatus for
            executing transaction processing relating to a
            customer, comprising:
            a main body (1); and
            a module (2) mounted removably on the main body (1)
            and constituted so as to be tamperproof;
            wherein the module (2) comprises an acquiring unit
            (14, 15) for acquiring secret information relating
            to the customer necessary for the transaction
            processing, an encrypting unit (18) for encrypting
            the secret information, and an interface (21) via
            which the module can connect to the main body so
            that the encrypting unit (18) can send the
            encrypted data to the main body; and
            the main body contains a control unit (13) for
            receiving the secret information encrypted by the

said encrypting unit and executing the transaction
processing using this secret information."

IV.   The following prior art document is cited in this
       decision:

D1:   US 6 065 679 A

V.   The examining division argued essentially as follows:

–   Document D1 did not disclose whether the non-
       tamperproof main body contained the control unit
       executing the transaction processing. Although D1
       was silent about the specific location of the
       transaction processing, it was reasonable to assume
       that this function was performed by the main
       processor of the core printed circuit board. The
       transaction terminal of D1 differed therefore from
       the terminal of claim 1 in that the control unit
       controlling the transaction processing was located
       in the tamperproof module and not in the non-
       tamperproof main body as specified in claim 1. This
       difference allowed, in the device of the invention,
       to update the functionality of the control unit
       executing the transaction processing without having
       to update the entire tamperproof module.

–   The objective problem could therefore be formulated
       as: How to allow an update of the functionality of
       the control unit controlling the transaction
       processing without having to upgrade the whole
       tamperproof module.

- When faced with the above problem the skilled person would have considered moving any entity which required frequent updates, but did not require a tamperproof environment, away from the tamperproof environment. Consequently, when adapting the terminal of Dl to solve the above objective problem, the skilled person would have considered locating the entities controlling the transaction processing outside of the tamperproof environment of the core unit.

VI.   The appellant applicant argued essentially as follows:

- The examining division's conclusion that the device of the present application did not involve an inventive step was based on hindsight. Already the statement of the problem identified by the examining division was in itself a big leap. The problem addressed by the invention should instead be formulated as: How to simplify updating the processor's software while maintaining the security of the device.

- Document Dl was a very long document whose main purpose was to provide a modular transaction terminal. Nevertheless, nowhere was any alternative location for any of its components mentioned. The main processor was the heart of the operation of the device controlling not only the transaction process, but also the complete functionality of the device (display, card reader, keypad, etc) and it was not obvious to remove it (together with the ASIC?) from the tamperproof area, as argued by the examining division.

–   The present invention had the remarkable technical
      effect that when an upgrade was needed it was not
      necessary to change the whole module having the
      tamperproof function; it was possible to upgrade
      only the control unit. This made it easy to extend
      the function of the control unit, taking advantage
      of its position in the main body.

Reasons for the Decision

1.   The appeal is admissible.

2.   *Document D1*

       Document D1 discloses a modular, portable transaction
       terminal comprising a tamperproof core unit 30 and a
       non-tamperproof communication unit 100. The core unit
       30 comprises *inter alia* a display 60, a keypad 42, a
       swipe style magnetic stripe reader 68, a smart card
       reader assembly 80, a core printed circuit board (PCB)
       46 and an interface connector 48, for allowing the core
       unit to interface with an exterior modular component.
       The core PCB 46 in turn hosts the main processor, an
       application specific integrated circuit (ASIC) 304 and,
       optionally, a high security second processor which
       together control the whole operation of the core unit
       30 (ie all applications running on the transaction
       terminal including the encrypting of the data) and,
       when attached, also the modular communication or
       printing unit in a master/slave mode (column 1, lines
       39 to 43; column 4, lines 20 to 31 and 50 to 59;
       column 5, lines 56 to 62; column 11, lines 30 to 39 and

50 to 53; column 12, lines 13 to 19; column 14, lines 5
to 43; column 22, lines 18 to 23; column 29, line 67 to
column 30, line 15; column 31, line 63 to column 32,
line 6; column 52, lines 25 to 37; column 61, lines 42
to 55; Figures 1, 4, 7, 8 and 13 to 15).

Although not specifically disclosed in D1, it is
reasonable to assume that also the transaction
processing is performed at the core PCB 46, since no
other processing unit capable of this function is
disclosed.

3.   The tamperproof core unit 30 and the non-tamperproof
      communication unit 100 of D1 correspond, respectively,
      to the tamperproof module 2 and to the non-tamperproof
      main body 1 of the present application.

4.   It is common ground that the transaction terminal
      device of claim 1 differs from the device of D1 in that
      the main body (ie the communication unit of D1)
      contains a control unit for receiving the secret
      information encrypted by the encrypting unit and
      executing the transaction processing using this secret
      information, since the transaction processing is
      performed in D1 by the core unit (ie the tamperproof
      module of the application).

5.   The examining division defined the objective problem
      addressed by this feature as "How to allow an update of
      the functionality of the control unit controlling the
      transaction processing without having to upgrade the
      whole tamperproof module".

The board, however, agrees with the appellant applicant
that this formulation of the objective problem is done
with hindsight and contains elements of the solution,
since in D1 there is no reference to a control unit
controlling the transaction processing. Therefore, the
objective problem addressed by the invention may be
formulated in more general terms as "How to simplify
updating the processor's software while maintaining the
security of the device", as suggested by the appellant
applicant.

6.   The solution to this problem is the recognition of the
      inventors that not all the processing had to be
      performed on a central processor, as in D1, where the
      core processor controls not only the transaction, but
      also the input/output devices, the encryption and all
      other applications running on the transaction terminal
      device. The recognition that not all control processes
      require a secure, tamperproof environment allows
      separating the tasks of the control unit into ones
      which require such an environment and others which do
      not.

      According to the invention the transaction processing
      does not require such a secure environment, since it
      handles only encrypted data that are secured by the
      encryption unit in the tamperproof module.

      This separation of tasks simplifies in turn the
      updating of the applications running on the control
      unit located in the non-tamperproof unit.

7.   The board considers that recognizing that not all
      processes had to be performed by a central, secured

C4138.D

control unit is not suggested by the disclosure of D1.
According to the so called "could-would" approach, the
skilled person could have separated the processes
running on the central control unit of D1, but the
board finds no incentive in the prior art that would
have induced the skilled person to do it. In particular,
since D1 discloses the optional use of a second secure
processor (the Dallas 5002 chip) that handles all
security functions (column 52, lines 25 – 37). However,
even in such case the main processor and the ASIC are
kept together with the second processor on the core PCB
46 within the tamperproof environment of the core unit
30.

8.   Consequently, the board finds that the portable
        transaction terminal device of claim 1 involves an
        inventive step within the meaning of 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 first instance with the
        order to grant a patent with the following documents:

        Claims:
             1 to 8 filed at the oral proceedings.

        Description:
             pages 1, 2, 6 to 10 as originally filed,
             pages 3 and 12 filed at the oral proceedings,
             pages 4, 5 and 11 filed with letter dated 2 July
             2010.

        Figures 1 to 7 as originally filed.

Registrar   Chair

S. Sánchez Chiquero   G. Eliasson