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

D E C I S I O N
of 27 October 2005

Case Number:	T 1107/02 - 3.5.01
Application Number:	97400664.5
Publication Number:	0809171
IPC:	G06F 1/00, H03M 11/00
Language of the proceedings:	EN

Title of invention:
Apparatus and method to provide security for a keypad
processor of a transaction terminal

Applicant:
Schlumberger Technologies, Inc.

Opponent:
-

Headword:
Keypad processor/SCHLUMBERGER TECHNOLOGIES

Relevant legal provisions:
EPC Art. 56

Keyword:
"Inventive step (yes, after amendment)"

Decisions cited:
-

Catchword:
-

Case Number: T 1107/02 - 3.5.01

D E C I S I O N
of the Technical Board of Appeal 3.5.01
of 27 October 2005

Appellant:	SCHLUMBERGER TECHNOLOGIES, INC. 825-B Greengrier Circle Chesapeake, VA 23320 (US)
Representative:	Cour, Pierre Axalto S.A. Intellectual Property Department 50, avenue Jean Jaurès F-92120 Montrouge (FR)
Decision under appeal:	**Decision of the Examining Division of the European Patent Office posted 5 April 2002 refusing European application No. 97400664.5 pursuant to Article 97(1) EPC.**

Composition of the Board:

Chairman:	S. Steinbrener
Members:	R. Wibergh
	G. Weiss

Summary of Facts and Submissions

I.   This appeal is against the decision of the examining
        division to refuse European patent application
        No. 97 400 664.5.

II.   According to the decision under appeal, the subject-
        matter of all 34 claims before the examining division
        was obvious.

III.   The examining division referred to the following prior
        art documents:

        D1: DE-A-41 26 760

        D2: EP-A-0 248 712

        D3: US-A-4 926 173

        D4: GB-A-2 190 775.

IV.   On 6 May 2002 the notice and grounds of appeal were
        filed and the appeal fee was paid. The appellant
        requested that the decision be set aside and a patent
        be granted based on the claims on file.

V.   By communication dated 18 April 2005 accompanying a
        summons to oral proceedings, the Board indicated that
        the subject-matter of claim 1 was not new.

VI.   Oral proceedings were held on 27 October 2005. In the
        course of the hearing the appellant filed a new set of
        claims 1 to 25.

VII.   Claims 1 and 16 read:

"1. A secured processor for use with a plurality of
data entry ports which receive data signals, the
secured processor comprising:
actual polling means operatively coupled to the
plurality of data entry ports for conducting actual
polling, the actual polling means providing an actual
polling means signal and monitoring data entry ports to
determine whether data signals are being received, the
actual polling means identifying the data entry ports
receiving data signals and generating an output signal
corresponding thereto; and
false polling means operatively coupled to the
plurality of data entry ports for providing a false
polling means signal to the plurality of data entry
ports for at least one of (i) producing a false
indication that a data signal is being received by at
least one of the plurality of data entry ports and (ii)
producing a false indication that actual polling of the
plurality of data entry ports is occurring;
wherein the actual polling means and the false polling
means include signal generators for providing actual
and false polling signals to the plurality of data
entry ports in the form of pulsed signals, each pulse
randomly varying in width."

"16. A method of providing a secured transmission of
actual data signals received by a keypad of a
transaction terminal to a processor which is external
to the transaction terminal, the method comprising the
steps of:

2950.D

a) polling the keypad by generating at least one pulse
signal to determine whether actual data signals are
being provided thereto;
b) polling the keypad by generating at least one pulse
signal to provide a false indication that at least one
of (i) actual data signals are being provided thereto
and (ii) actual polling of the transaction terminal is
occurring; and
c) encoding the actual data signals and transmitting
the encoded data signals to the external processor/,/
wherein the pulses randomly vary in width."

Independent claim 20 was directed to a transaction
terminal comprising a secured processor circuit.

VIII.   The appellant requested that the decision under appeal
        be set aside and a patent be granted on the basis of
        claims 1 to 25 filed at the oral proceedings.

IX.   At the end of the oral proceedings the Board announced
        its decision.

Reasons for the Decision

1.   *Admissibility of the appeal*

        The appeal meets the requirements referred to in
        Rule 65(1) EPC and is, therefore, admissible.

2.   *Amendments*

        The main amendment to the three independent claims is
        the addition of the feature that the pulses of the

actual and false polling means signals vary randomly in
width. This feature was included in claims 13, 21 and
22 of the application as originally filed, referred to
at various places in the description, and illustrated
in figure 2C (box 63) and figure 2D (boxes 100,102).
Thus, there is no objection against these claims under
Article 123(2) EPC.

3.   *Clarity, support*

The independent claims are regarded as fulfilling the
requirements of Article 84 EPC (but see paragraph 8
below with respect to Rule 29(7) EPC).

4.   *The invention*

As explained in the description of the present patent
application (columns 1 and 2), transaction terminals
are known which require a user to enter a personal
identification number (PIN) via a keypad. Such
terminals have the disadvantage that it is possible for
an electronic eavesdropper to attach electrical tapping
connections to the keypad conductors in order to
monitor when a circuit connection is made by a key
depression (e.g., when PIN data is entered). It is
therefore possible for the electronic eavesdropper to
obtain PIN information from the transaction terminal
and to use that data to execute a fraudulent
transaction. A known solution to this problem is to use
polling signals which serve not only to sample the
keypad in order to detect key actuations ("actual
polling") but also to mask the actual polling signals
("false polling"). The invention aims at further
reducing the likelihood of successful electronic

eavesdropping by varying the duration of the actual and false polling pulses in a random manner.

5.   *The prior art*

According to D2, held to be the closest prior art document, actual polling signals applied in sequential order to the rows of a keyboard matrix are detected on a randomly selected column in a receiving mode. False polling signals are simultaneously applied to the other columns in order to produce false indications that data signals are being received on these columns. A false polling signal is also applied to the receiving column in case it is determined that no genuine signal is present. This signal is necessarily somewhat shorter than the others, a difference which could at most be detected with the aid of sophisticated equipment. In another mode (see figure 5, case dx) actual key interrogation is inhibited and false polling pulses of the same width are simultaneously applied to a line and to each of the columns so that key activation is simulated.

6.   *Novelty*

Claim 16, which is the most general claim, now includes the feature that the pulses (of the actual and false polling signals) vary randomly in width. In the decision under appeal (point 6.4), the examining division cited passages in D1 (column 2, lines 5 to 11), D3 (column 3, lines 18 to 28; column 6, lines 14 to 19) and D4 (page 2, lines 26 to 30) to demonstrate that in particular length modifications of polling signal pulse were known. However, in D1 and D4 it is apparently the

2950.D

simulated key actuations whose duration varies, not the individual polling pulses. Moreover, in D1 the variation is between devices rather than between pulses. In D3 a pulse pattern varies but not the pulse length. The Board further notes that in D2 the period of the false polling pulses can assume two (slightly) different values, which is not the same thing as a pulse having a randomly varying width.

It follows that the invention as set out in claim 16 is new (Article 54 EPC). The same applies to claims 1 and 20.

7.   *Inventive step*

7.1   The purpose of varying the pulse width of the actual and false polling signals is to confuse an eavesdropper, who will not be able to detect a sampling pattern based on the pulse width, the pulses assuming a noise character (cf. column 6, lines 1 to 6; column 10, line 58 to column 11, line 5; column 13, lines 42 to 50). Starting out from D2, the technical problem can be seen in modifying the known circuit in a way which makes eavesdropping even more difficult.

7.2   The examining division, citing the passages from D1, D3 and D4 identified in paragraph 6 above, held that modifications of orders, forms, lengths and frequencies of the polling signals were measures familiar to the skilled person. The Board agrees that it is generally known in this technical area to generate various kinds of random signals in order to confuse eavesdroppers. It is for example pointed out in D2 that it is advantageous if the controlling microcomputer operates

in as random a fashion as possible (column 8, lines 25
to 27). The invention is however not just concerned
with this general principle but with its particular
application to the length of the polling pulses. The
question is whether the skilled person, having regard
to the relevant prior art, would have thought of using
randomly varying polling pulses in order to obtain some
advantage.

7.3   It is clear that false polling signals, to serve their
        purpose, should in principle be indistinguishable from
        the actual polling signals. According to the prior art
        documents, in so far as they at all specify the shape
        of the shapes, all polling pulses are made as identical
        as possible (D2, figure 5; D4, figure 2). D2 is
        especially clear in this respect. According to this
        document, after a key associated with a certain column-
        row combination has been explored and found not to be
        activated, a false polling signal is immediately
        generated in order to minimise the difference in
        duration between this signal and the other false
        polling pulses simultaneously applied to the other
        columns (paragraph bridging columns 6 and 7). Against
        this background it is difficult to see why the skilled
        person would have thought of using anything but
        identical pulses for the actual and false polling
        signals. Although D2 states that the processes should
        preferably be performed randomly, an important aim in
        this document is in fact to obtain identical pulses.
        This strongly suggests that the statement was
        insufficient to lead the skilled person to the present
        invention.

7.4   With the benefit of hindsight it may naturally be
        argued that the skilled person would have realised that
        random variations of the pulse width are at least as
        effective as perfect uniformity to ensure the anonymity
        of the pulses and that such variations offer the
        additional advantage of increased overall complexity of
        the signals. But this would be a mere allegation
        amounting to little more than an explanation of the
        present invention, and appears less convincing than the
        observations above directly based on the prior art.

7.5   Thus, the subject-matter of claim 16 involves an
        inventive step (Article 56 EPC). The same applies to
        claims 1 and 20.

8.   *Remittal*

        The patent application must still be examined with
        respect to the other requirements of the Convention. It
        is for example noted that the claims do not contain
        reference signs (Rule 29(7) EPC) and that the
        description has not yet been adapted to the new claims.
        This final examination is left to the examining
        division.

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 for further prosecution.

The Registrar: The Chairman:

M. Kiehl   S. Steinbrener

2950.D